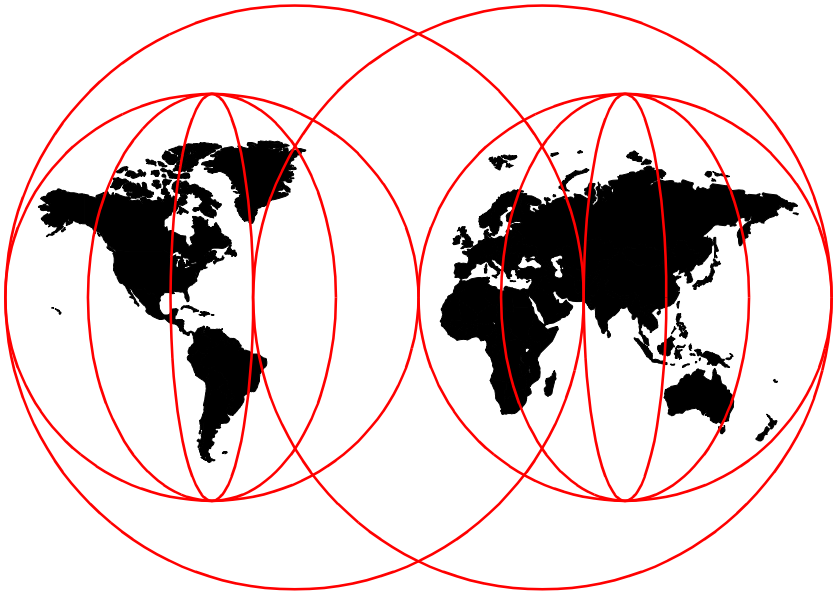
AS/400 IBM Network Station: Techniques for Deployment in a WAN

Fant Steele, Nick Harris, Joan Barrett, Hernan Coronel,
Andy Grant, Yudhi Haryadi, Gerri Passe



International Technical Support Organization

http://www.redbooks.ibm.com

SG24-5187-00

SG24-5187-00

International Technical Support Organization

AS/400 IBM Network Station: Techniques for Deployment in a WAN

March 1999

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix D, “Special Notices” on page 285.

First Edition (March 1999)

This edition applies to IBM Network Station Manager Program Version 1 Release 3, Program Number 5648-C05, and OS/400 Version 4 Release 3.

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. JLU Building 107-2
3605 Highway 52N
Rochester, Minnesota 55901-7829

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© Copyright International Business Machines Corporation 1999. All rights reserved
Note to U.S Government Users – Documentation related to restricted rights – Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Contents

Figures ix

Tables xiii

Preface xv
The Team That Wrote This Redbook xv
Comments Welcome xvii

Chapter 1. Introduction 1
1.1 IBM Network Station Family Overview 1
1.2 What is New in IBM Network Station Manager for AS/400 Release 3 . . 2
1.2.1 National Language Support 4
1.2.2 Network Station Manager Group Support 5
1.2.3 Separation of Servers 6
1.2.4 Broadcast Boot for AS/400 10
1.2.5 Converged 5250/3270 Emulators 12
1.2.6 VTxxx Telnet Emulation 13
1.2.7 Support for Twinax-enabled IBM Network Stations 14
1.2.8 Streaming LPR/LPD Support 15
1.2.9 ICA Client Protocol 17
1.2.10 Lotus eSuite Workplace 17
1.2.11 JVM 1.1.4 and JIT 18
1.2.12 NC Navigator Browser Enhancements 18
1.2.13 Inventory Server for AS/400 19
1.2.14 Full-Screen (Kiosk) Solutions Support 20
1.2.15 DHCP Support 21
1.3 Local versus Remote Users 21
1.4 Initialization Options for Remote Sites 22
1.4.1 Remote Boot Servers 22
1.4.2 IBM 2212 Nways Access Utility 26
1.4.3 Flash Memory Card Boot 28
1.4.4 Network Station Terminology 30

Chapter 2. Planning Considerations 33
2.1 Where You Are Currently 33
2.2 What You Are Likely to Have Now 35
2.3 What You Are Trying to Achieve 35
2.4 Capacity 37
2.5 Performance 37
2.5.1 Network Station Network Data 38
2.6 Performance Conclusions 52

© Copyright IBM Corp. 1999

2.7 Problem and Change Management 55
2.8 Migration Considerations 55
2.9 Roaming. 56
2.10 Slow Link Boot versus Flash Card Peer Boot 56
2.11 CISC and RISC Co-existence. 57
2.12 Printing with Your IBM Network Station 58
2.12.1 Configuring Printers on an AS/400 System 58
2.12.2 Configuring Basic Printer Scenarios 60
2.12.3 Printer Administration Techniques 61

Chapter 3. Using Flash Cards with the Network Station 63
3.1 Flash Card Support 64
3.1.1 Flash Card Sizing 65
3.1.2 Flash Card Management 66
3.1.3 Separation of Servers, Authentication Login, and the Flash Card 67
3.1.4 Hardware Considerations 68
3.2 Booting from a Flash Card with 5250, 3270, and VTxxx Support 69
3.2.1 Scenario Objectives 69
3.2.2 Scenario Advantages 70
3.2.3 Scenario Disadvantages. 70
3.2.4 Scenario Network Configuration 71
3.3 Creating A Flash Card 72
3.3.1 Verifying Prerequisites 73
3.3.2 Creating a Flash Card Boot Image 73
3.3.3 Task Summary 73
3.3.4 Creating a Separate Configuration File. 76
3.3.5 Testing the Boot Image from the AS/400 System 77
3.3.6 Verifying Functionality 79
3.3.7 Accessing the Local File Manager and NFS 81
3.3.8 Formatting the Flash Card 82
3.3.9 Loading the Image onto the Flash Card 84
3.3.10 Booting the IBM Network Station Using the Flash Card 89
3.3.11 Verifying Functionality 93
3.3.12 House Keeping. 94
3.3.13 Flash Card Boot Summary 95
3.4 Peer Booting with 5250, 3270, and VTxxx Support. 96
3.4.1 Scenario Objectives 97
3.4.2 Scenario Advantages 97
3.4.3 Scenario Disadvantages. 98
3.4.4 Network Configuration Scenario 98
3.5 Task Summary 99
3.5.1 Planning Considerations. 99
3.5.2 Modifying Existing Flash Boot Network Station Configuration . . 100

3.5.3 Creating a Peer Boot Configuration File 101
3.5.4 Configuring the Peer Boot Network Station 102
3.5.5 Verifying Functionality 104
3.5.6 Peer Boot Summary 105

Chapter 4. Remote Servers and Split Boot Servers 107
4.1 Terminology for this Chapter 107
4.2 Boot Sequence 107
4.3 Split Boot Feature 108
4.4 Server Consolidation 109
4.4.1 Scenario Objectives 109
4.4.2 Scenario Overview 110
4.4.3 Consolidating Servers 111
4.5 Roaming Feature 120
4.5.1 Managing User Configurations at Each Remote Site 121
4.5.2 Centralized versus Distributed 124

Chapter 5. Twinax Attachment of Network Stations 127
5.1 Use of Twinax Attached Network Stations 127
5.2 AS/400 Software Requirements 128
5.3 AS/400 Hardware Requirements 128
5.4 Basic IP over Twinax Scenario 128
5.4.1 Scenario Overview 129
5.4.2 Scenario Objectives 129
5.4.3 Scenario Advantages 129
5.4.4 Scenario Disadvantages 129
5.4.5 Scenario Network Configuration 129
5.4.6 Task Summary 130
5.4.7 Defining a TCP/IP Address Range 130
5.4.8 Configuring and Starting the IBM Network Station 130
5.4.9 Configuring an AS/400 IP Interface 132
5.4.10 Testing Connectivity 139
5.4.11 Summary 139
5.5 Transparent Subnet Masking 140
5.5.1 Twinax Transparent Subnetting Example 141
5.6 Advanced IP over Twinax Scenario 144
5.6.1 Scenario Overview 144
5.6.2 Scenario Objectives 144
5.6.3 Scenario Advantages 145
5.6.4 Scenario Disadvantages 145
5.6.5 Scenario Network Configuration 145
5.6.6 Task Summary 146
5.6.7 Planning the TCP/IP Addressing Scheme 146

5.6.8 Configuring and Starting the IBM Network Station 147
5.6.9 Configuring an AS/400 IP Interface. 147
5.6.10 Testing Connectivity 153
5.6.11 Summary 153
5.7 Twinax IBM Network Station with Local DHCP Server Scenario 154
5.7.1 Scenario Overview 154
5.7.2 Scenario Objectives 154
5.7.3 Scenario Advantages 154
5.7.4 Scenario Disadvantages. 154
5.7.5 Scenario Network Configuration 155
5.7.6 Task Summary 156
5.7.7 Planning the TCP/IP Addressing Scheme. 156
5.7.8 Configuring the DHCP Server As1 for Twinax Support 157
5.7.9 Configuring and Starting the IBM Network Station 164
5.7.10 Testing Connectivity 170
5.7.11 Summary 171
5.8 Twinax IBM Network Station with a Remote DHCP Server Scenario 171
5.8.1 Scenario Overview 171
5.8.2 Task Summary 172
5.8.3 Configuring the Local DHCP Configuration File on As1 173
5.8.4 Power on the IBM Network Station 175
5.8.5 Manually Changing the Auto Created TCP/IP Interface 177
5.8.6 Configuring and Starting BOOTP/DHCP Relay Agent. 177
5.8.7 Changing the DHCP Server Configuration 180
5.8.8 Configuring the Twinax Subnet Address Pool 187
5.8.9 Starting the IBM Network Station 190
5.8.10 Testing Connectivity 190
5.8.11 Summary 190
5.9 Twinax IBM Network Station with Remote Boot Server. 191
5.9.1 Scenario Overview 192
5.9.2 Scenario Objectives 192
5.9.3 Scenario Advantages 193
5.9.4 Scenario Disadvantages. 193
5.9.5 Scenario Network Configuration 193
5.9.6 Task Summary 194
5.9.7 Configuring the DHCP Server on As1 194
5.9.8 Ensuring the Proper TCP/IP Servers are Started on As2 204
5.9.9 Configuring and Starting the Twinax IBM Network Station 205
5.9.10 Testing Connectivity 208
5.9.11 Summary 208

Chapter 6. Problem Determination 209
6.1 Viewing the IBM Network Station Console Log 209

6.1.1 Accessing the System Log Using TELNET 209
6.1.2 Accessing the System Log Using the Console Manager 211

Chapter 7. Replicating a Remote Boot Server Environment 213
7.1 Centralized Authentication Server 213
7.1.1 IBM Network Station Manager Replication to Remote Server . . 214
7.2 Decentralized Authentication Server. 217
7.2.1 IBM Network Station Manager Replication to Remote Server . . 218
7.3 Summary 224

Chapter 8. Using a Network Station to Access Mail 225
8.1 POP3 Mail Configuration 225
8.1.1 Basic POP3 Configuration 225
8.2 Lotus eSuite Workplace 228
8.2.1 Starting eSuite on the Network Station 229
8.2.2 eSuite Mail Configuration on Network Station 231
8.3 NC Navigator Access 234
8.3.1 Starting NC Navigator. 234
8.3.2 Configuring NC Navigator to Access e-mail 236
8.4 Domino Access 239
8.4.1 Deciding What to Specify for Server Characteristic. 239
8.4.2 Avoiding Conflicts between AS/400 HTTP Server and Domino . 242
8.4.3 Accessing the Web Browser 243
8.4.4 Terminal Server Edition and Citrix MetaFrame Overview 248
8.4.5 Connecting IBM Network Station to Windows Terminal Server . 249
8.4.6 Lotus Notes 4.6a Basic Installation on Windows Terminal Server 250

Appendix A. Flash Card Scenarios 255
A.1 Support for 5250, 3270, and VTxxx Emulation 255
A.2 Support for 5250, 3270, and VTxxx with Fonts. 258
A.2.1 The Flash.nsm File Additions to Support Local Font Storage 261
A.2.2 The Peer.nsm File Additions to Support Local Font Storage 261
A.3 Support for NC Navigator with Java Virtual Machine 262
A.4 Support for ICA Client 264
A.5 Java Application Support 265

Appendix B. Executable Module Descriptions 267
B.1 Module Information 267

Appendix C. 5500 Express IP Control Unit 271
C.1 5500 Express IP Control Unit 271
C.1.1 Twinax Client Connection Requirements 272
C.2 Connection Configurations of the 5500 Control Unit 273

C.2.1 WAN Configuration Data 277
C.2.2 ISDN Modems 278
C.3 5500 Control Unit and TCP/IP LAN Concepts 278
C.3.1 Installing the IBM 5500 into an Existing Network 279
C.4 Optimizing Twinax Performance for the Client Workstation 282
C.5 Using the 5500 Control Unit as a Network Station Boot Server 283

Appendix D. Special Notices 285

Appendix E. Related Publications 289
E.1 International Technical Support Organization Publications 289
E.2 Redbooks on CD-ROMs 289
E.3 Other Publications 290

How to Get ITSO Redbooks 291
How IBM Employees Can Get ITSO Redbooks 291
How Customers Can Get ITSO Redbooks 292
IBM Redbook Order Form 293

Index 295

ITSO Redbook Evaluation 299

Figures

1. Roaming User Example 8
2. Separation of Servers - Load Balancing Example 9
3. Changing TFTP Attributes for Subnet Broadcast Boot 11
4. Enabling Subnet Broadcast Boot for IBM Network Stations 11
5. Remote Boot Servers Example 25
6. IBM 2212 Access Utility 27
7. Remote Site - Flash Memory Card Peer Boot Example 30
8. Network Components that May Exist in Your Organization 35
9. Network Station Implementation 36
10. Possible Network Station Printing Scenarios 59
11. Flash Card Support for Emulators from a Remote Location 70
12. Remote Flash Card Enabled IBM Network Station Topology Diagram . . . 72
13. Example Flash.nsm File 77
14. Console Log Example: Loading the 5250 Emulator from the Test Image Directory 81
15. Updated Example of the Flash.nsm File 91
16. Console Log Example: Loading the 5250 Emulator from the Flash Card . 94
17. Peer Boot Topology Diagram 97
18. Peer Boot Detailed Network Topology 99
19. Example Peer.nsm File 101
20. Peer Boot Loading of the 5250 Emulator from the Flash Card 105
21. Boot Sequence 108
22. Distributed Server Topology 110
23. Consolidated Server Topology 111
24. Users and User Group 112
25. User ITSCIDGRPA 113
26. Group Creation 114
27. User’s Attributes (Part 1 of 2) 115
28. User’s Attribute (Part 2 of 2) 115
29. Paste Group’s Configuration Files 117
30. Resulting Group’s Configuration Files 118
31. Roaming Example 120
32. Fully Centralized Configuration 122
33. Remote Reboot with Centralized Configurations 123
34. Distributed Model 124
35. Centralized Model 125
36. TCP/IP Network Topology for Basic IP over Twinax Scenario 130
37. Display of QSYSOPR Message Queue on AS/400 System 132
38. Display of QHST Log on the AS/400 System 133
39. Configuration Status Display of Automatically Created QTDL Descriptors134

© Copyright IBM Corp. 1999

40. QTDL824300 Line Description. 134
41. Automatically Created Device Type 5150 under CTL01 135
42. Adding IP Interface for QTDLC824300 Line Description 136
43. Starting the Interface for the QTDLC824300 Line Description 136
44. Configuration Status of QTDL824300 Line, Controller, and Device 137
45. Updated 5150 Device Description 138
46. BOOTP Table Entry for Twinax IBM Network Station 138
47. Display of BOOTP Table Entry 139
48. Transparent Subnetting Example 141
49. Subnet Mask Boundaries and Address Ranges 141
50. Transparent Subnetting Twinax Scenario with Class C TCP/IP Address 143
51. Transparent Subnetting Class C Address Example. 143
52. Network Topology for Advanced IP over Twinax Scenario 145
53. Applying Subnet Mask to Carve a Contiguous Range for Twinax Subnet147
54. Display of QSYSOPR Message Queue on AS/400 System 148
55. Configuration Status Display of Automatically Created QTDL Descriptors148
56. Configuration Status Display of Automatically Created Display Device. . 149
57. Adding IP Interface for QTDLC827500 Line Description 150
58. Starting the Interface for the QTDL827500 Line Description 150
59. TCP/IP Interface Status Display 151
60. Configuration Status of QTDL Descriptors. 151
61. Updated 5150 Device Description 152
62. BOOTP Table Entry for Twinax IBM Network Station 152
63. Display of BOOTP Table Entry 153
64. Network Topology for Local DHCP Server Scenario 155
65. Applying Subnet Mask to Carve a Contiguous Range for Twinax Subnet157
66. AS/400 Operations Navigator - Configure DHCP Server. 158
67. AS/400 Operations Navigator - Selecting Network 158
68. AS/400 Operations Navigator - Selecting Network Servers. 159
69. AS/400 Operations Navigator - Selecting TCP/IP Servers 159
70. AS/400 Operations Navigator - DHCP Configuration 160
71. DHCP Server Configuration Twinax Subnet 160
72. DHCP Twinax Address Pool Range 162
73. Twinax Attached DHCP Options Configuration 163
74. AS/400 Operations Navigator - TCP/IP Server Status. 164
75. QTDLxxxxxx Line, Controller, and Device Configuration Status 167
76. QTDLxxxxxx Line Description 167
77. Device Type 5150 under CTL01 168
78. TCP/IP Interface for the Local Workstation Controller 169
79. TCP/IP Interface Updated with an Associated Local Interface Value . . . 170
80. Using Remote DHCP Server to Configure Twinax IBM Network Stations 172
81. AS/400 Operations Navigator DHCP Configuration for Twinax Subnet on As1 System 174

82. AS/400 Operations Navigator - TCP/IP Server Status. 175
83. Automatically Created QTDL Descriptors 176
84. CFGTCP Option 1 Display Showing the TDLC Interface. 176
85. TCP/IP Interface Updated with an Associated Local Interface Value . . . 177
86. AS/400 Operations Navigator - Configuring BOOTP/DHCP Relay Agent 178
87. BOOTP/DHCP Relay Agent Configuration 179
88. AS/400 Operations Navigator - TCP/IP Server Status. 180
89. Applying Subnet Masks 181
90. AS/400 Operations Navigator - Creating New Subnet in DHCP 182
91. DHCP Configuration 183
92. DHCP Configuration 184
93. DHCP Configuration - Forming a New Subnet Group 185
94. DHCP configuration - New Subnet Group Properties 186
95. DHCP Configuration - Selection of Subnets for New Subnet Group 187
96. DHCP Configuration - Showing Contents of Subnet Group. 187
97. DHCP Configuration - New Subnet Group. 188
98. DHCP Configuration - Remote Twinax IP Address Pool 189
99. Operations Navigator - DHCP Configuration Display Showing Subnet Groups 190
100.Twinax Attached Network Station Obtaining Network Configuration . . . 192
101.Network Topology for Remote Boot Server Scenario 193
102.Operations Navigator - DHCP Twinax Subnet Properties. 195
103.DHCP Configuration - Defining TFTP Server 196
104.DHCP Configuration - Option 211 Configuration Protocol Template . . . 197
105.DHCP Configuration - Option 212 Terminal Server Template 197
106.DHCP Configuration - Option 213 Configuration File Path Template . . . 198
107.DHCP Configuration - Option 214 Protocol to Use Template 198
108.DHCP Configuration - Viewing Available Options. 199
109.DHCP Configuration - Adding Tag 211 Configuration Protocol. 200
110.DHCP Configuration - Adding Tag 212 Terminal Server. 201
111.DHCP Configuration - Adding Tag 213 Configuration File Path 202
112.DHCP Configuration - Adding Tag 214 Protocol. 203
113.Operations Navigator - Modified DHCP Configuration Display 204
114.Netstat *CNN Display Showing Active TCP/IP Servers 205
115.Operations Navigator - TCP/IP Server Status Display 205
116.Set Network Parameters Display (Before Bootup) 206
117.Set Configuration Parameters Display (Before Bootup) 207
118.Sample Messages on Network Station during Startup 207
119.Set Network Parameters Display (After Bootup). 208
120.Set Configuration Parameters Display (After Bootup). 208
121.Windows 95 RUN Dialog Box 209
122.TELNET Terminal Preferences. 210
123.TELNET Terminal Connection Dialog Box 210

124.Console Log Example 211
125.Replicating Remote Boot Servers - Centralized Authentication Server . 214
126.Replicating Remote Boot Servers - Decentralized Authentication 218
127.Customize System Default Menu Bar Buttons 220
128.Add Custom NC Navigator Button to System Default Menu Bar. 220
129.Add 3270 Menu Bar Button to Group Grp3270's Preference Settings . . 221
130.Option 12 of the CFGTCP Menu - Change TCP/IP Domain 225
131.DNS Server Configuration. 226
132.Display of Host Table Entry. 226
133.Directory Entry for POP User - General Information 226
134.Mail Service Level - System Message Storage (Preferred Address) . . . 227
135.Add Directory Entry - SMTP Name for User 227
136.eSuite Workplace Desktop 229
137.Menu Content Defaults Display. 230
138.QSYSOPR Message Queue Showing Start of eSuite Server. 231
139.eSuite Mail Configuration 232
140.eSuite Inbox 233
141.Network Settings - System Defaults Display. 235
142.Main Dsplay of the NC Navigator Browser 236
143.NC Navigator: Mail & News Preferences Display 237
144.NC Navigator Mail Inbox 238
145.User ID and Password Prompt 245
146.Views Display 246
147.Web Mail Inbox 247
148.Configuring an ICA Client 250
149.Lotus Notes Workstation on IBM Network Station 253
150.Transition from SNA to TPC/IP with 5500 Control Unit. 271
151.IBM 5500 in an Express Environment. 274
152.IBM 5500 with a Combination of Media Types 275
153.Asynchronous Dialup Connectivity 276
154.Frame Relay Connectivity. 277
155.5500 Subnet Example. 280
156.Example of a Network before Installing the IBM 5500 281
157.Example of a Network after Installing the IBM 5500 282

Tables

1. Applications and Printer Data Streams 16
2. Elements Loaded to a Network Station (MB) 39
3. Time (Seconds) to Perform Hardware Test 43
4. Kernel/Configuration Initialization Time 45
5. Kernel/Configuration Initialization Time 45
6. Kernel/Configuration Initialization Time 46
7. Kernel/Configuration Initialization Time 46
8. Kernel/Configuration Initialization Time 47
9. Kernel/Configuration Initialization Time 47
10. Load Times (Seconds) 49
11. Load Times (Seconds) 49
12. Load times (Seconds) 51
13. LAN to Twinax Throughput 52
14. Desired Print Scenarios 60
15. PCMCIA Flash Card Part Numbers 64
16. Kernel and Application Program Sizes 65
17. Network Station Local File Manager Commands. 88
18. Options for DCHP Server-to-Server. 163
19. Options and Values 189
20. Module Information 267
21. The Defaults.dft File. 284

© Copyright IBM Corp. 1999

Preface

Gain an edge implementing an IBM Network Station solution in a Wide Area Network (WAN). This redbook offers a number of alternative implementation techniques that demonstrate the IBM Network Station's flexibility and rapid deployment capabilities.

As you read this book, you find valuable information about running IBM Network Station with Network Station Manager Program Release 3 (NSM). This redbook also discusses the details of the new functions provided with NSM Release 3 and subsequent Program Temporary Fixes (PTFs). These functions include Broadcast Boot for AS/400, enhanced converged 3270/5250 emulators, VTxxx Telnet emulation, streaming LPR/LPD print support, ICA Client protocol, Lotus eSuite Workplace, integrated 40-bit NC Navigator browser, DHCP support, and Flash memory cards. In addition, this redbook offers an introduction to the 2212 Nways Access Utility and the 5500 Express IP control unit.

This redbook is intended for the I/T professional who has customers with existing IBM Network Stations and are planning to implement the new functions available with Network Station Manager Program Release 3. It also targets those professional that are planning to replace non-programmable terminals (NPTs) with IBM Network Stations.

The Team That Wrote This Redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization Rochester Center.

Fant Steele is an Advisory ITSO Specialist for AS/400 in the International Technical Support Organization, Rochester Center. He writes extensively and teaches IBM classes worldwide on many areas of AS/400 communications technologies and e-business. He spent eight years as an instructor and developer for the AS/400 communications and programming curriculum of IBM Education and Training. Prior to joining IBM in 1989, he worked on S/36 to AS/400 code conversion, VM/MVS systems programming, and applications programming for the manufacturing industry.

Nick Harris is an Senior Systems Specialist for the AS/400 in the International Technical Support Organization, Rochester Center. He writes and teaches IBM classes worldwide on areas of AS/400 System Design, Business Intelligence, and Database. He spent 11 years as a System

© Copyright IBM Corp. 1999

Specialist in the United Kingdom AS/400 Business. Prior to joining IBM, he worked for the Ministry of Defense as a Mechanical and Electrical Design Engineer.

Joan Barrett is an Advisory I/T Availability Professional in the AS/400 Software Support Center in Canada. She has worked for IBM for 10 years. Over the past five years, she worked in the communications group within the AS/400 platform. In the previous five years, she worked as a Customer Service Representative in the Mid-range systems field. Her areas of expertise include AS/400 communications, and specifically TCP/IP and SNA protocols, workstation controllers, and network stations.

Hernan Coronel is an I/T Specialist in Argentina. He has been working for IBM for four years and spent the last three years as a system administrator for the Bueños Aires e-business center. He holds a degree in Computer Science from University CAECE. His areas of expertise include TCP/IP networking and IBM Network Stations.

Andy Grant is a communications specialist working for IBM Managed Operations Group in New Zealand. He has eight years of experience with IBM mid-range systems, communication, and PC connectivity. His main area of expertise is the design, implementation, and support of large, multi-platform networks. This includes host inter-connectivity and desktop-to-host configuration and trouble shooting over a variety of communication protocols.

Yudhi Haryadi is an I/T Service Specialist working for IBM Product Support Service in Indonesia. He has four years of experience with IBM Network hardware device and software, operating systems, and network operating system. His main area of expertise is in the design, implementation, and support of small to large customer networks.

Gerri Passe is a Senior Technical Sales Specialist with the IBM North America Advanced Technical Support Organization. During the last 18 months, she has worked with AS/400 customers and business partners in the area of IBM Network Station implementation and has also presented at a number of internal and external technical conferences. In addition, she has seven years prior experience as an AS/400 Systems Engineer and Services Specialist working with Client Access and AS/400 Internet connectivity. Prior to working in the AS/400 environment, she was an IBM S/390 Systems Engineer.

Thanks to the following people for their invaluable contributions to this project:

Ray Romon, Network Station Development Manager
Chuck Carmack, Network Station Development
Dave Limpert, Network Station Software Architect
AJ Meyer, Network Station Development
Ron Stevenson, Network Station Performance
IBM Rochester

Marc Pamely, Product Engineer
Buz Stepanek, 5500 Product Management
IBM Charlotte

Comments Welcome

Your comments are important to us!

We want our redbooks to be as helpful as possible. Please send us your comments about this or other redbooks in one of the following ways:

- Fax the evaluation form found in “ITSO Redbook Evaluation” on page 299 to the fax number shown on the form.
- Use the online evaluation form found at: `http://www.redbooks.ibm.com`
- Send us a note at the following address:

  `redbook@us.ibm.com`

Chapter 1. Introduction

Although IBM Network Stations can be locally attached to your AS/400 using twinax, Ethernet, or Token Ring using TCP/IP. This redbook focuses on implementing IBM Network Stations at your *remote* sites. In addition, this redbook assumes that you have some familiarity with IBM Network Stations. This chapter includes a brief overview of IBM Network Stations, a summary of the IBM Network Station Manager for AS/400 Release 3 enhancements, and an introduction to several methods available for deploying IBM Network Stations throughout your AS/400 wide area network.

1.1 IBM Network Station Family Overview

The IBM Network Station family provides you with an alternative for your business desktop. Traditionally, your choice was limited to either non-programmable terminals (NPTs) or personal computers. NPTs are very simple to install and maintain. However, they often lack the flexibility and function needed by users. Although PCs are very flexible and functional, they can end up being under-utilized and installation and ongoing support requirements can be substantial. The IBM Network Station family consists of network computers that are designed to combine some of the best characteristics of NPTs and PCs, which reduces complexity and cost by placing their management on central servers. IBM Network Stations can be booted from an IBM AS/400, RISC System/6000, S/390 or NT PC server when the appropriate software is installed.

All three models of the IBM Network Station allow you to access existing applications on your network, as well as corporate intranets and the Internet. In addition, the IBM Network Station takes advantage of leading edge technologies, such as Java.

The IBM Network Station Series 100, often referred to as the *access network computer*, is best suited to provide access to applications residing on servers in your network. The Series 100 model offers:

- Access to multiple servers (IBM and others)
- Ability to run Windows applications using multi-user implementations of Windows NT
- Support for 5250, 3270 and VTxxx terminal applications
- Access to applications on AIX and UNIX servers using X-Windows server support
- Benefit from significant processing power of your server

© Copyright IBM Corp. 1999

The IBM Network Station Series 300, the *Internet network computer,* is an ideal solution when your users spend a lot of time on your corporate intranet or the Internet, as well as access server based applications. In addition to providing the same Series 100 capabilities listed above, the Series 300 can run simple or entry level Java applets and applications.

The *Java network computer*, as the IBM Network Station Series 1000 is called, offers the robust support that allows your users to access business-critical applications and/or personal productivity tools that take advantage of Java. The IBM Network Station Series 1000 allows you to:

- Run Java applets and applications directly on the IBM Network Station
- Run Windows applications using a multi-user implementations of Windows NT
- Access multiple servers (IBM and others), including corporate intranet and Internet servers, using Web browsers
- Access applications using 5250, 3270 and VTxxx emulation
- Work with applications on AIX and UNIX servers using X-Windows server support
- Capitalize on the combined processing power of your servers and the Series 1000 to optimize network resources and put the right application in the right place

For additional information about IBM Network Stations and the IBM Network Station Manager for AS/400 R3 product, refer to the manuals *IBM Network Station Manager Installation and Use,* SC41-0664, and *IBM Network Station Use*, SA41-0036. You may also find an earlier redbook, *AS/400 - IBM Network Station - Getting Started*, SG24-2153, useful. However, it does not contain Release 3 information. These manuals can be found on-line at the Web site: www.ibm.com/nc/pubs

1.2 What is New in IBM Network Station Manager for AS/400 Release 3

The IBM Network Station Manager for AS/400 licensed product provides several major functions: 5250 emulation, 3270 emulation, the Java Virtual Machine, and the IBM Network Station Manager *program*. This program is an easy-to-use browser based application that enables a single systems administrator to set up and configure all IBM Network Stations in their enterprise. It lets you centrally create and manage user-specific desktop environments and access privileges to accommodate different user needs. The IBM Network Station Manager provides centralized control for all IBM Network Station applications and access to server resources, such as printers. The system administrator can access the IBM Network Station

Manager from any location on their TCP/IP network using an appropriate browser.

In June of 1998, a new release with significant enhancements to IBM Network Station Manager for AS/400 became available. Major enhancements included in Version 1 Release 3 are:

- National Language Support
- Network Station Manager group support
- Separation of servers
- Broadcast boot for AS/400
- Enhanced converged 3270/5250 emulators
- VTxxx Telnet emulation
- Support for the new twinax-enabled IBM Network Station model 341
- Streaming LPR/LPD print support
- ICA Client protocol
- Lotus eSuite Workplace
- Java Virtual Machine (JVM) 1.1.4
- Java Just-In-Time compiler (Series 1000 only)
- Integrated 40 bit NC Navigator browser
- Inventory Server for AS/400
- Full-screen solutions (kiosk) support
- DHCP support

In addition, a number of enhancements for Release 3 of IBM Network Station Manager for AS/400 were recently made available through PTFs (program temporary fixes). These PTFs, which can be obtained by ordering the AS/400 group PTF SF99082, include support for the following:

Flash memory cards

Allows you to store the IBM Network Station operating system and applications in specific third-party Series D Type II PCMCIA memory cards and boot a remote IBM Network Station locally or through peer (*buddy*) boot. Please refer to Chapter 3, “Using Flash Cards with the Network Station” on page 63 for more details.

Multiple serial ports

Allows the use of additional peripheral devices by extending the IBM Network Station’s serial interface from a single native serial port to multiple serial ports through the use of a third-party Type II PCMCIA Card. One, two, or four additional ports can be added to attach serial devices to the IBM Network Station.

Touch-sensitive display

Provides support for IBM and selected third party touch-sensitive displays which allows users to select on-display options by placing a

finger directly on the display and dragging or clicking objects as if you were using a mouse. With this free enhancement and a touch-sensitive display, the IBM Network Station can be the client for a broad range of applications requiring read-only access to data, from kiosks in shopping malls to hospitals, museums, and libraries.

PCMCIA on Series 1000

Enables the use of a Type II PCMCIA card slot on the IBM Network Station Series 1000 after it has been installed. Unless you received one of the few early Ethernet IBM Network Station Series 1000s that were shipped with a PCMCIA slot, you must order this chargeable PCMCIA Adapter (part number 07L8336) option by contacting your IBM representative or an IBM Business Partner.

Note: PTF Enhancements

Additional information on the above four enhancements can be found online at the Web site at: www.pc.ibm.com/networkstation/solutions/product.html.

Note

If you want to learn more about Release 3 of IBM Network Station Manager, an educational CD entitled *IBM Network Station Manager Release 3: A Tutorial* is now available. This training CD includes a wide range of cross platform, technical topics pertaining to Network Station implementation. It can be ordered through the IBM Publications department as kit number SK3T-3024-01. In the United States, publications can be ordered by calling: 800-879-2755.

1.2.1 National Language Support

Release 3 of IBM Network Station Manager for AS/400 supports the IBM Network Station across all geographies. The National Language Support (NLS) enablement includes support for more than 30 languages. This allows users around the world to use language-specific keyboards, read on-display system messages and, in some cases, read instruction manuals in their native languages.

For additional information about National Language Support, refer to the manual *IBM Network Station Manager Installation and Use,* SC41-0664, and in the online help text of the IBM Network Station Manager program.

1.2.2 Network Station Manager Group Support

Previous releases of IBM Network Station Manager for AS/400 provided default *system, user* and *workstation* level settings. These settings which define the IBM Network Station's user desktop environment, can be changed by the system administrator (and in some instances the user). For example, the administrator could:

- Configure hardware and workstation settings on a system-wide and user level. Preference settings include:
  - Specifying primary mouse buttons (left or right-handed).
  - Setting mouse pointer speeds.
  - Updating boot monitor version.
  - Selecting screen saver, desktop background, and more.
- Configure access to applications on a system-wide and user level:
  - 5250 emulator to access IBM AS/400 applications.
  - 3270 emulator to access IBM S/390 applications.
  - X-Windows to access graphical UNIX applications.
  - Web browsers to access the Internet and corporate intranets.
  - Desktop (Window Manager) to customize the user's display interface.
  - Applet viewer to run Java applets and applications.
  - Windows based applications (running on a multi-user system).
- Configure system wide and user level start up settings such as:
  - Programs to automatically load frequently used applications, such as 5250 emulation
  - Menu items to provide point-and-click access to other applications using menu bar buttons

In addition to the above capabilities, Release 3 of IBM Network Station Manager for AS/400 allows you to define *group* level settings. Although this significant function proves useful to all customers, it is particularly helpful if you are setting up and managing larger numbers of IBM Network Stations throughout your enterprise. For example, you may have customer service personnel in your headquarters and in a remote site who share similar desktop and application needs. Group support allows you to set up a *custserv* group which defines a common desktop environment for all the users in that group, rather than having to define the same settings for each user.

1.2.3 Separation of Servers

Several IBM Network Station Manager for AS/400 server functions that were previously bundled can now be *split* and installed on multiple servers. This allows you to balance network traffic, if desired. Balancing network traffic enables IBM Network Station end users to access their normal desktop when they are away from their regular server.

To use separation of servers, you must install the zero-charge IBM Network Station Manager Release 3 licensed program on each computer system providing one of the server functions discussed in this topic (except for the system acting only as a BOOTP/DHCP server). If used on the AS/400 system, the BOOTP or DHCP server function is actually provided by TCP/IP. Also, DHCP server support on an AS/400 system requires Version 4 Release 2 or later. On any one specific computer system, IBM Network Station Manager Release 3 can be used to perform *more than one* server role. It is also important to remember that, if desired, the server functions can be split across different supported computer systems. For example, your V4R2 AS/400 with IBM Network Station Manager for AS/400 Release 3 can provide the base code, terminal configuration, and authentication server functions and have another server (such as, AS/400, NT or RISC System/6000) act as the DHCP server. A brief description of each server role follows.

BOOTP/DHCP Server

The BOOTP or DHCP server provides the IBM Network Station with information such as its IP address, the base code server address, and the address of the terminal configuration server. Unlike BOOTP, the DHCP server allows you to *dynamically* assign IP addresses to clients upon request. Refer to the manual, *IBM Network Station Manager Installation and Use,* SC41-0664, for examples on how to accomplish load balancing by specifying a different address for the base code server and configuration server. This manual and others are online at: www.ibm.com/nc/pubs. As mentioned previously, the IBM Network Station Manager for AS/400 product does *not* need to be installed on the AS/400 DHCP server that is servicing DHCP and BOOTP clients.

Base Code Server

The IBM Network Station Manager for AS/400 product on this server provides the operating system and the application programs that are downloaded to the IBM Network Stations during initialization. This server is not used to configure IBM Network Stations.

Terminal Configuration Server

The IBM Network Station Manager program on this server provides terminal-based configuration settings. The IBM Network Station Manager program manages these settings. Examples of terminal configuration settings are a printer that is attached to the network station, or the network station's keyboard language. The address of the terminal configuration server is the same as the address of the base code server by default. The inventory server (AS/400 only) runs on this server.

Authentication Server

The IBM Network Station Manager program on this server provides user authentication (when the user logs on) and user-based configuration settings. The IBM Network Station Manager program manages these settings. Examples of what you can configure on this server are users auto-start sessions (for example, 5250 sessions) or users browser preferences. The IP address of the authentication server is the same as the address of the base code server by default. You may use a different authentication server by clicking on the **Roam** button on the IBM Network Station logon display and then entering the server's name or IP address. A technique for automating the use of a different server for authentication is discussed in Chapter 4., "Remote Servers and Split Boot Servers" on page 107.

You may have already thought of several uses for this new separation of server function. The following are instances in which multiple servers can prove to be an advantage:

- As shown in Figure 1 on page 8, users from Dallas are visiting your central site in Rochester and want to sign on and receive the same desktop environment that they have at home using the roaming function. User can click on the **Roam** button on the IBM Network Station logon display and then enter the name or IP address (10.2.1.2) of their Authentication Server in Dallas. At that time, their own preferences are downloaded over the TCP/IP network to the IBM Network Station (10.1.1.20) from the Dallas system and the users see their *home* desktop.

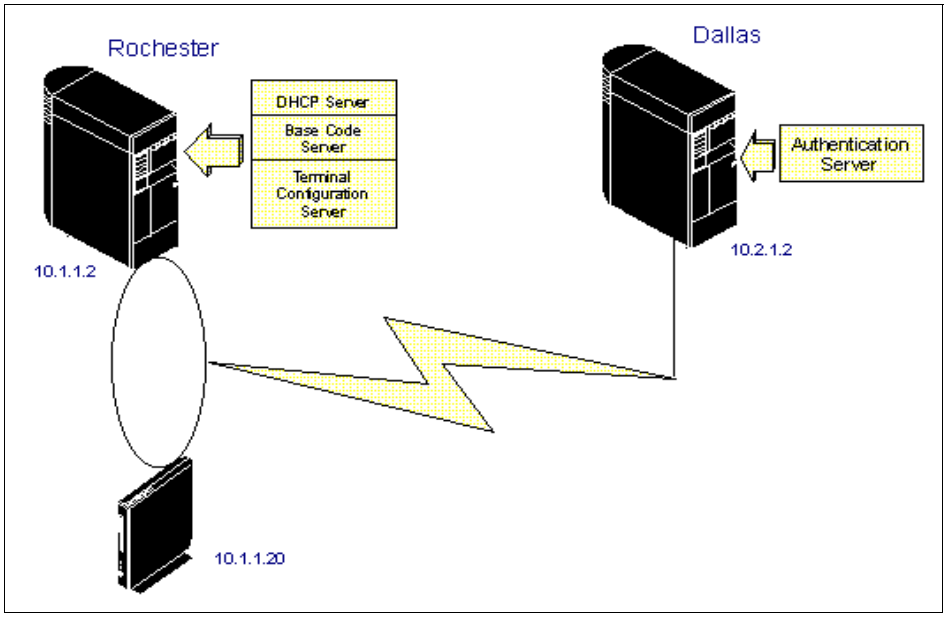


Figure 1. Roaming User Example

- Figure 2 on page 9 shows how the separation of servers function might be used to reduce network congestion if all IBM Network Stations are powered on at 8:00 on Monday morning. In this case, separation of servers is used to split the server functions across multiple systems. For example, one AS/400 (10.1.1.2) provides both the authentication and terminal configuration server functions and the PC server (10.2.1.2) is the DHCP server. In addition, there are two AS/400s (10.3.1.2 and 10.4.1.2) acting as base code servers. This distributes copies of the large executable files (operating system and applications) across servers. Although the PC server providing the DHCP server function only, does *not* require IBM Network Station Manager Release 3. It *must* be installed on the other systems that are providing the base code, terminal configuration and authentication server functions.

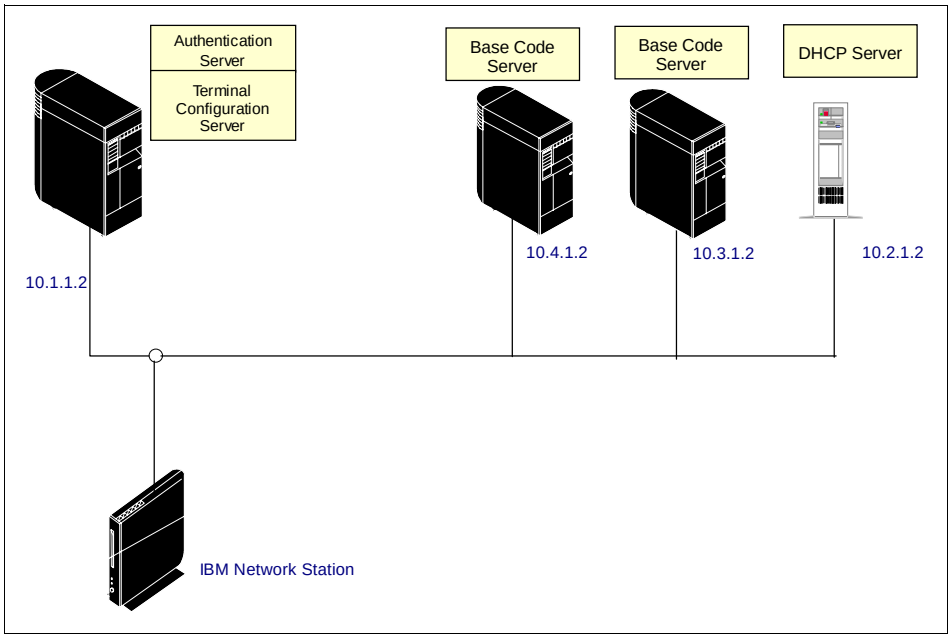


Figure 2. Separation of Servers - Load Balancing Example

For additional information on how to use the separation of servers function to enable user roaming and provide load balancing, refer to the manual *IBM Network Station Manager Installation and Use,* SC41-0664. This manual and others are available on-line at the Web site: www.ibm.com/nc/pubs

Split Boot server is discussed in Chapter 4, “Remote Servers and Split Boot Servers” on page 107.

Important

All servers must be running IBM Network Station Manager Version 1 *Release 3* to use separation of servers. However, as mentioned above, an exception to this is the BOOTP/DHCP server. A DHCP or BOOTP server does *not* need the IBM Network Station Manager licensed product installed as long as it is not providing any of the other separation of server functions.

1.2.4 Broadcast Boot for AS/400

The broadcast boot support in IBM Network Station Manager for AS/400 Release 3 provides the capability to boot multiple Network Stations on the same subnet. This broadcast boot is performed in parallel through a single transmission. In situations where large numbers of IBM Network Stations start up at the same time, heavy network usage or boot storms can result. Trivial File Transfer Protocol (TFTP) Subnet Broadcast (or Broadcast Boot) is a solution to balancing your network traffic during these boot storms because it reduces LAN usage and AS/400 CPU utilization.

The reason boot storms may occur is that the AS/400 server is trying to deliver the boot kernal file to every IBM Network Station in the network. When the TFTP Subnet Broadcast option is enabled and multiple IBM Network Stations request their boot files, the server stages the boot file download and only distributes it *once*. Essentially, the first Network Station on the subnet which requests its boot file becomes the *master*. When other IBM Network Stations on the same subnet request their boot files, the *master* serves them. It passes on the files received during its initialization. The *master* continues its role until it has completed its initialization. Once completed, the *master* role passes to the next IBM Network Station that requests the kernal file. This sequence continues until new IBM Network Station assumes the role of *master*.

You must enable the TFTP Subnet Broadcast option on both the AS/400 server and the IBM Network Station. By default, the TFTP Subnet Broadcast option is enabled on your AS/400. However, as shown in Figure 3 on page 11, you should verify this by typing in CHGTFTPA and ensure that the *Enable Subnet Broadcast* parameter value is set to *YES. You must then start up the Network Station Manager from your browser, and as shown in Figure 4 on page 11, select the Hardware/Workstation Setup Task to change the *Enable Broadcast Boot* to *Yes.*

```
                        Change TFTP Attributes (CHGTFTPA)

Type choices, press Enter.

Autostart server . . . . . .   *yes, *NO, *SAME
Enable subnet broadcast . . *YES       *YES, *NO, *SAME
Number of server jobs:
  Minimum  . . . . . . . . . .   2             1-20, *SAME, *DFT
  Maximum  . . . . . . . . . .   6             1-250, *SAME, *DFT
Server inactivity timer  . . . .   30          1-1440, *SAME, *DFT
ASCII single byte CCSID:
  Coded character set identifier   00819       1-65532, *SAME, *DFT
Maximum block size . . . . . .   8192          512-65464, *SAME, *DFT
Connection response timeout  . .   60          1-600, *SAME, *DFT
Allow file writes  . . . . . .   *NONE         *DFT, *NONE, *CREATE...
Alternate source directory . . .   '*none'



                                                                    More...
F3=Exit    F4=Prompt    F5=Refresh    F12=Cancel    F13=How to use this display
F24=More keys
```

Figure 3. Changing TFTP Attributes for Subnet Broadcast Boot

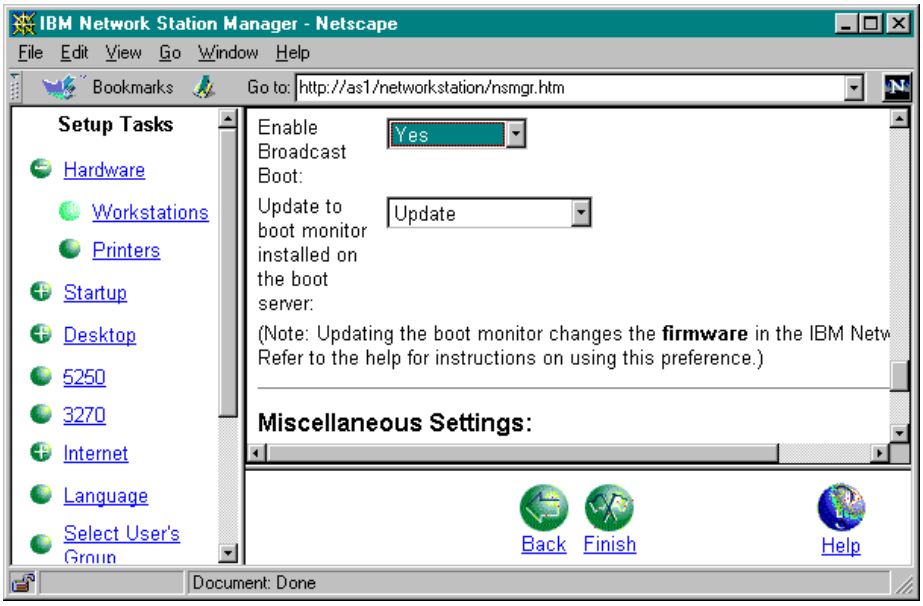


Figure 4. Enabling Subnet Broadcast Boot for IBM Network Stations

Important

Before you use TFTP Subnet Broadcast, you *must* ensure that certain PTFS are installed on every AS/400 in your network. Please refer to the manual *IBM Network Station Manager Installation and Use,* SC41-0664, for the most current list of PTFs. These PTFs prevent unpredictable results, including possible data loss. This manual can be found online at the Web site: www.ibm.com/nc/pubs

1.2.5 Converged 5250/3270 Emulators

The 5250 and 3270 emulators have been enhanced to provide additional function and user interface consistency. Key enhancements in the 5250 emulator include 3489 Image/Fax support (5250 display and print of color JPEG, monochrome image and fax), user customizable keypads and Hot Spot highlighting. In addition to the customizable keypads, and the Hot Spot highlighting, the 3270 emulator has been enhanced to include functions which were previously available in the 5250 emulator such as:

- Local display print
- Record and playback macros
- Auto signon
- Emulator menu bar customization
- Initial window location and size selection
- Status line (Operator Information Area)
- Copy, cut, and paste using edit menu
- Miscellaneous preferences

Although the 5250 and 3270 emulators have separate executables, they share the same source and have the following additional enhancements in common:

- IBM Network Station Manager program support for Group level preferences
- Emulator display print to network printer through *remote printer* configuration in IBM Network Station Manager program
- Any key can be used to start a playback file
- Keyboard remapping files can be named (helps administrator when setting up multiple default remapping files)
- Support for 40+ 3270/5250 emulator session languages (available languages can be seen by selecting the Language Setup Task in the IBM

Network Station Manager program and selecting the LANG parameter pull-down list).

- Emulator menu bar or pull downs, dialogue boxes, online help, keyboard remapping, color mapping, record/playback, and so on, are now translated into many languages (a list of available languages can be seen by selecting the Language Setup Task in the IBM Network Station Manager program and then clicking on the pull down list for the LC_MESSAGES parameter).
- Operator Information Area (OIA) now includes a communication status field, which may show some of the following messages:
  - COMM655: Waiting for telnet option negotiation (normal to see this temporarily displayed)
  - COMM656: Initializing TCP/IP socket interface
  - COMM657: Resolving host name of Telnet server
  - COMM658: Initializing TCP connection for Telnet
  - COMM659: TCP attachment has been lost
- Single Key Print
- Automatic Communication Error Recovery
- Graphics Print Support
- Display Name enhancements
- TN3270E

Note

Although it was available in the previous release, it is significant that Network Station 5250 sessions can have static display names. More details are available in the Network Station Manager or 5250 online help text.

1.2.6 VTxxx Telnet Emulation

This new support allows IBM Network Station users to access systems which require VTxxx clients. The VTxxx Telnet client supports Latin-1 character sets for locales other than English in the host session windows. However, its MRI (Machine Readable Information) is English only. In this context, English only MRI means that anything outside of the actual host application supplied content is in English. For example, the VTxxx help text and error messages only display in English. In addition, the VTxxx client does not provide as many functions as the 5250 and 3270 emulation clients. For example, the VTxxx client does not provide a graphical keyboard or color remapping utility or a

record and playback function. However, hand editing of VTxxx keyboard mapping files is available. After hand editing a VTxxx mapping file, you can use the new group support (see Section 1.2.2, “Network Station Manager Group Support” on page 5) by putting the file into the group’s proper file path/directory on the authentication server and then using the Network Station Manager program to associate the desired users with that group. Also, although the VTxxx client supports display printing, its display print function is implemented differently than in the 5250 and 3270 clients.

As with 5250 and 3270 sessions, a VTxxx emulation session can be set up for your users from the IBM Network Station Manager program using the Programs or Menus setup task. This new VTxxx client is designed to provide VT320 support. The VTxxx client will work in your environment if you can answer *yes* to the question, *Can this application work with a real VT320 terminal?* Telnet does not equate to direct connect, for example, TCP/IP encapsulation. In addition to VT320 and Xterm, the following are also supported:

- VT300
- VT200
- VT220
- VT102
- VT100

1.2.7 Support for Twinax-enabled IBM Network Stations

Release 3 of IBM Network Station Manager for AS/400 provides support for the recently announced twinax enabled IBM Network Station Model 341. This IBM Network Station offers the same functional capabilities as the other Series 300 IBM Network Station models *without* requiring you to change your twinax wiring. Now it is easier for you to:

- Use corporate intranets and the Internet using the NC Navigator for IBM Network Station browser.
- Enjoy the cost-effectiveness of non-programmable terminals (NPTs) with simultaneous access to corporate applications using 5250, 3270, VTxxx and X-terminal emulation.
- Allow access to Windows based applications by running a multi-user NT version of software, such as WinCenter from NCD, Inc., on an attached PC Server or Windows NT Server V4.0 -Terminal Server Edition and Citrix MetaFrame running on a PC server or on the AS/400 IPCS (Integrated PC Server).

You can set up your network environment on your AS/400 server to allow some or all of the IBM Network Stations of use twinax connectivity. Beginning

with OS/400 V4R2, a special type of TCP/IP can run over a twinax network. In addition, you must create a relationship between the workstation controller and a TCP/IP interface. A TCP/IP interface is needed to identify your workstation controller to your AS/400 server and IBM Network Stations. Each TCP/IP interface *must* have a unique IP address. The IP addresses for twinax IBM Network Station models are assigned by the TDLC (Twinax Data Link Control) component on the AS/400 system.

The IBM Network Stations attached to the workstation controller act as if they are a TCP/IP subnet. Therefore, the subnet represented by the TCP/IP interface has a network address and a subnet mask. The twinax subnet also uses a Domain Name Server (DNS), just like any other subnet.

The twinax interface works like any other local area network (LAN) interface. It interacts with the other LAN cards on your AS/400 system in much the same way as a router's multiple interfaces work together. The interface passes packets from your twinax Network Stations to a LAN card on the same server. The LAN card forwards the packets to a router and out to the Internet.

Appendix B in the *IBM Network Station Manager Installation and Use,* SC41-0664, can assist you in planning for and implementing twinax attached IBM Network Stations. In addition, Chapter 5, “Twinax Attachment of Network Stations” on page 127 in this redbook discusses the implementation of twinax IBM Network Stations.

1.2.8 Streaming LPR/LPD Support

Printing capabilities have been significantly enhanced in Release 3 of IBM Network Station Manager for AS/400 as a result of adding support for the TCP/IP LPR/LPD protocol (RFC 1179). LPR is an acronym for Line Printer Requester and LPD is an acronym for Line Printer Daemon. This protocol enables the IBM Network Station to function as a print client or print server. This support also includes LPR/LPD streaming support, which is a draft extension to RFC 1179.

If LPD on the server does not support streaming (AS/400 system has supported this since V2R2), then LPR on the IBM Network Station attempts to build a complete spool file using available memory on the Network Station.

This new printing support allows local client applications on the IBM Network Station to send print jobs to remote print servers or remote printers. In addition, remote print clients are able to send print jobs to either the serial port or parallel port on the IBM Network Station. However, more importantly, the AS/400 (at V4R2 or later) system has the capability to transform one data

stream into another. If you are using IBM Network Station applications that generate PostScript data, but you only have a PCL type printer attached to your IBM Network Station, the print request can be sent to the AS/400 system, transformed from PostScript to PCL, and routed back to the IBM Network Station attached PCL printer.

You can configure printers for your IBM Network Stations with the IBM Network Station Manager program unless the data stream generated by the Network Station application does not match a datastream that your printer understands. Table 1 describes which data streams the common IBM Network Station applications produce. If your Network Station application does not produce a datastream that your printer understands, you must send the print job to an AS/400 server to *transformed* it into the datastream of your choice.

Table 1. Applications and Printer Data Streams

Application	**Data streams**
5250 Emulator	Postscript, ASCII, PCL
3270 Emulator	Postscript, ASCII, PCL
VTxxx Emulator	ASCII
NC Navigator browser	Postscript
Java Applications	Postscript
Lotus eSuite Workplace	Postscript

For example, in the previous release, you needed a Postscript capable printer *directly* attached to your IBM Network Station if you wanted to print from your NC Navigator browser session. In Release 3, you can continue to print to your local Postscript printer. Now, you can also route non-Postscript output through the AS/400 system (V4R2 required) where it is transformed to Postscript and then routed back to your locally attached Postscript printer. In addition, assuming the administrator has enabled access to the printer, you can choose to send the non-Postscript output to a network printer located on your network.

For comprehensive information on configuring and utilizing printers with your IBM Network Stations, refer to the manual, *IBM Network Station Manager Installation and Use,* SC41-0664 and the redbook, *IBM Network Station Printing Guide*, SG24-5212. Both of these technical publications can be viewed online at the Web site at: as400service.ibm.com

Important

Transforming print jobs requires *OS/400 Version 4 Release 2 or later.* Because the host print transform takes place on the server, the AS/400 system resources are utilized.

1.2.9 ICA Client Protocol

In addition to the previously available X11 protocol support, Release 3 also allows you to use the ICA protocol to access Microsoft Windows based applications running on a server. ICA (Independent Computing Architecture) is a general purpose presentation services protocol that provides access to Windows based applications; ICA also provides support for low bandwidth connectivity.

If any of your IBM Network Station users requires access to Windows based programs like personal productivity applications, a multi-user NT server solution, such as Microsoft Windows NT 4.0, Terminal Server Edition and Citrix MetaFrame must be used.

IBM Network Stations booting from an AS/400 with Release 3 of IBM Network Station Manager installed continues to access Windows applications running on a multi-user NT 3.5.1 based WinCenter Pro solution provided by Network Computing Devices (NCD) Incorporated. If you use the t Windows NT Server 4.0, Terminal Server Edition and Citrix MetaFrame products, your IBM Network Station users can access WIndows-based applications using the ICA (Independent Computer Architecture) protocol (see Section 1.2.9, “ICA Client Protocol” on page 17 for more information on ICA). You can use the WinCenter for MetaFrame product from Network Computing Devices, Inc. (when available) if you want to continue using the X.11 protocol to access Windows-based applications. The WinCenter for MetaFrame product also provides increased system administration support. Additional details for these products are found at their respective Web sites:

- www.ncd.com
- www.microsoft.com
- www.citrix.com

1.2.10 Lotus eSuite Workplace

Lotus eSuite Workplace is an innovative new class of productivity software designed especially for the network computing environment. The eSuite Workplace provides users with a simple, intuitive interface to an integrated

set of Java applets that provide a basic set of functions such as email, calendar, word processing, spreadsheet, address book and presentation graphics in a single product. IBM Network Station Manager for AS/400 Release 3 allows you (the system administrator) to easily set the eSuite Workplace product as the default desktop. The eSuite Workplace (with or without the IBM Network Station menu bar) can be selected through the IBM Network Station Manager program by changing a setting in the *Startup Menus* setup task. An IBM Network Station Series 1000 with 64 MB is required to use Lotus eSuite Workplace. If the system that used to serve eSuite Workplace to the IBM Network Station Series 1000s is an AS/400 system, it must have the following installed:

- OS/400 V4R2 OS/400 V4R2 or V4R3 & latest CUM Tape
- 5769-JV1 - AS/400 Developer Kit for Java
- 5648-C05 - IBM Network Station Manager Release 3.0
- PTF SF49066 (5769-SS1 V4R2 only) for Security enhancements

Additional installation information on Lotus eSuite Workplace can be found in the *readme* documents located on the Web site:
service.boulder.ibm.com/nc/as400/index.html

1.2.11 JVM 1.1.4 and JIT

In previous releases of IBM Network Station Manager for AS/400, a Java Virtual Machine is included with Release 3. However, in this release of IBM Network Station Manager for AS/400, an updated Java Virtual Machine (JVM 1.1.4) is included. To improve performance, the Just-In-Time (JIT) Compiler allows an application's or applet's Java bytecode to be compiled as it is downloaded into the IBM Network Station Series 1000. Currently, the JIT is most effective in improving compute-intensive and string manipulation operations.

1.2.12 NC Navigator Browser Enhancements

Previously, the browser was ordered and installed as a separate product. However, in Release 3 of IBM Network Station Manager for AS/400, the NC Navigator browser (40 bit encryption version) is *integrated* into the base product. This fully compatible subset of the popular Netscape Navigator 3.0 browser is an upgrade of the existing Navio NC Navigator browser currently available. This new integrated 40 bit NC Navigator or the separate 128 bit NC Navigator replaces the earlier Navio NC Navigator in Release 3 of the IBM Network Station Manager. In fact, the earlier Navio NC Navigator (5648-B10 or 5648-B20) and the IBM Network Station browser (5648-B08 or 5648-B18) will *not* run with Release 3 of IBM Network Station Manager for AS/400.

Release 3 also provides a number of other enhancements to the NC Navigator browser such as:

- Mail client function enables a user to send and receive e-mail using a POP3 (Post Office Protocol V3) server.
- News Reader function enables a user to read news items on an NNTP (Network News Transfer Protocol) server.
- The Navigator enables printing to remote printers on the network.
- Localized versions enable French, German, and Korean (in addition to English) languages.
- The browser enables invoking the 3270 emulator and Telnet from the browser.

As mentioned previously, if you prefer to use the 128 bit encryption version of NC Navigator (available only in the United States or Canada), then you must order it and install it as a separate AS/400 product. The product number for the 128 bit version of NC Navigator for IBM Network Stations is 5648-C20. You can order this product by calling 1-800-879-2755 (USA only) and referring to the CD/publication collection kit SK3T-3020.

1.2.13 Inventory Server for AS/400

The new inventory server allows you to collect information about your IBM Network Stations. Every IBM Network Station contains a simple network management protocol (SNMP) agent in its operating system. As a result, an SNMP manager at a central location can communicate and exchange information with the IBM Network Station agent. You can use this information to manage your network environment. SNMP is an industry-standard protocol for network management.

The AS/400 inventory server collects and stores the hardware information in a DB2 for AS/400 database. Some examples of the information which can be collected include the following:

- Burnt-in MAC address of the IBM Network Station
- IBM Network Station memory size
- IP address of the BOOTP or DHCP server
- Network Station's IP address
- Network Station network interface type (Ethernet, Token Ring, Twinax)
- Boot monitor version installed

For additional information about how to start the inventory server, what data can be collected, and how it can be retrieved from the database using SQL statements, refer to the manual *IBM Network Station Manager Installation and Use,* SC41-0664. If you want to use SQL queries to retrieve information

from the database, you must have IBM DB2 Query Manager and SQL Development Kit for AS/400 installed.

Note

If you decide to use the new separation of servers function, the hardware inventory server must run on the server providing the Terminal Configuration server function.

1.2.14 Full-Screen (Kiosk) Solutions Support

In specific environments, you may want the IBM Network Station, after power is turned, to automatically start up a particular application like 5250 or 3270 emulation without requiring the entry of a user ID and password on the login display. For example, a public library may want to limit and simplify the user interface by allowing a user access to only a library book search application from the IBM Network Station. Another common environment where full-screen support can be useful is in a shopping mall kiosk.

Although a full-screen solution was feasible with the prior release of IBM Network Station Manager, it required you to hand edit a number of files and the login/authentication was bypassed rather than hidden or suppressed. Release 3 of IBM Network Station Manager allows you to *suppress* the login and provides an easier implementation because the Network Station Manager program is primarily used.

Essentially, this solution involves the creation of a special kiosk user ID for each particular appearance of a full-screen application. The following full-screen solution applications are supported:

- 5250 Emulator
- 3270 Emulator
- PC desktop
- Unix Common Desktop Environment
- NC Navigator

In addition, these special kiosk user IDs, passwords and the associated IBM Network Stations IP addresses or names must be placed in an encoded kiosk user ID file on the server. As a result, when those specified IBM Network Stations are powered on, the login display is suppressed and the preferences of the corresponding kiosk user ID are used to automatically bring up the appropriate full-screen desktop.

Details on implementing full-screen solutions are found online at the Web site: www.ibm.com/nc/pubs in the *Advanced User Information* section.

1.2.15 DHCP Support

An AS/400 with TCP/IP and OS/400 Version 4 Release 2 or later installed can be configured to act as a DHCP server. DHCP (Dynamic Host Configuration Protocol) allows a server to automatically provide IP addresses and configuration information to clients without needing to manually keep track of client MAC addresses. (MAC is an acronym for media access control; each IBM Network Station has a unique *burnt-in* MAC address.)

Release 3 of IBM Network Station Manager for AS/400 provides the support that allows IBM Network Stations to use an AS/400 DHCP server. Chapter 5, “Twinax Attachment of Network Stations” on page 127 discusses implementing twinax IBM Network Stations in an AS/400 DHCP server environment. For additional information about planning and configuring DHCP, refer to the redbook, *AS/400 TCP/IP Autoconfiguration: DNS and DHCP Support*, SG24-5147, and the manual, *TCP/IP Configuration and Reference,* SC41-5420. These manuals are found online at the Web site: as400service.ibm.com

Important

Release 3 of IBM Network Station Manager for AS/400 has *increased* memory requirements for the IBM Network Stations. Use the manual, *IBM Network Station Manager Installation and Use,* SC41-0664 to estimate and verify the IBM Network Station memory size required for your environment.

1.3 Local versus Remote Users

Are your users local or remote? A site that is located 500 miles away from your central AS/400 would be considered remote. However, it is possible that your friend who works in shipping across the street is really a remote user. One definition of a remote AS/400 user is *someone* who is using communications facilities to connect their workstation to the AS/400 system rather than directly attaching to the AS/400’s Local Area Network (using token ring or Ethernet) or to an AS/400 twinax workstation controller.

For example, your friend in shipping across the street may be connected to the AS/400 over a communications line due to local regulations or other reasons. In addition, perhaps users attached to the Token Ring LAN in the

headquarters building one block away are actually remote since that Token Ring LAN is connected to the AS/400 LAN through a remote bridge. As you can see, it is very important to understand your existing network. If a current network diagram does not already exist, it is very important to create one before implementing network computers.

Sample network diagrams are found throughout other chapters in this redbook. In addition, other manuals which contain TCP/IP planning information, including sample network diagrams, are the following:

- *TCP/IP Fastpath Setup*, SC41-5430
- *TCP/IP Configuration and Reference,* SC41-5420 (see Chapter 3 "Configuring TCP/IP" for a sample network diagram)
- *IBM Network Station Manager Installation and Use,* SC41-0664 (see the Chapter 1 topic "What Do I Need to Know About TCP/IP Networks" for sample network diagrams)

1.4 Initialization Options for Remote Sites

As previously mentioned, IBM Network Stations can be locally attached to an AS/400 boot server using Token Ring, Ethernet or twinax connectivity. In fact, some of you may already have locally attached IBM Network Stations in your enterprise. In addition, you may also have users in remote sites who could benefit from having IBM Network Stations. You may be wondering how to best implement them in your remote sites. Although it is technically possible to boot remote IBM Network Stations over a wide area network, it is *not* advisable to do because boot up time can range from 10 to 20 minutes over a 56 KB connection. (Remember, the operating system kernel and other files are being downloaded from the boot server to the IBM Network Station.) Therefore, we recommend that you boot remote IBM Network Stations from a remote boot server, through local Flash card peer boot or through the new IBM 2212 Access Utility solution. Each of these options are outlined in the following sections and the remote boot server and local Flash card peer boot options are discussed in subsequent chapters. The 2212 Access Utility was not yet available when this redbook was being written. Therefore, a chapter detailing its implementation could not be included. However, an IBM redbook discussing the IBM 2212 Access Utility is planned for availability in 1999.

1.4.1 Remote Boot Servers

One of the advantages of the IBM Network Station is that it can boot from a properly configured AS/400, RS/6000, S/390, or PC (NT) server. As a result, a potential boot server may already exist at your remote site. For example,

you may have already installed or plan to install distributed AS/400 systems in some or all of your remote sites for various reasons. These remote AS/400 systems can provide users with local access to applications like Domino and also act as a boot server.

A remote AS/400 boot server option is one which provides a high degree of flexibility and function for the current andl future needs of your remote users . However, as with any installation, time and effort is required to plan for and implement these remote boot and application servers. The level of effort varies, depending on the number of remote sites, how autonomous the sites are, and the applications deployed.

In determining whether a remote boot server is the right solution for your remote IBM Network Station end users, consider the following items:

- Is there an AS/400 system or other system capable of being a boot server in the remote site?

  If you have a system at a remote site, is it capable of running IBM Network Station Manager for AS/400 Release 3?

  For example, an AS/400 system at V3R7 or later can run Release 3 but several functions such as DHCP support and print transformation require V4R2. In addition, OS/400 V3R2 systems can *only* run Release 2.5 of IBM Network Station Manager for AS/400. Therefore, all of the new R3 enhancements, like separation of servers and group support, are not available. In addition, do you already have TCP/IP installed and configured in your remote site? As expected, implementing TCP/IP requires planning and effort. For several good resources to start with, refer to the manuals *TCP/IP Fastpath Setup*, SC41-5430 and the *IBM Network Station Manager Installation and Use,* SC41-0664.

- If there is a potential boot server at the remote site, is it already fully utilized?

  Perhaps you already have an AS/400 system at your remote site that will soon be upgraded to V4R2 and you need to add 20 new IBM Network Station users who primarily need access to new AS/400 based applications. You need to determine whether the existing AS/400 system is already running at capacity (for example, disk and CPU) to see whether it can handle the 20 new IBM Network Station users. Depending on your environment, you may be using the Performance Tools/400 product to gather performance data and then using the BEST/1 capacity planning tool. In addition to the potential TN5250 load of the new users, you should also consider that some AS/400 CPU is needed during the initialization of the IBM Network Stations. However, due to their low power requirements,

the general recommendation is to leave the IBM Network Stations powered on. Therefore, the AS/400 CPU required for Network Station boot up will most likely be needed only occasionally. On the other hand, your site may have different policies or habits regarding the powering off of desktop workstations on a daily or weekly basis. In these cases, it is more critical to have adequate CPU to handle the more frequent IBM Network Station initialization. Refer to Section 2.4, “Capacity” on page 37 for additional details about capacity planning.

- Are you already considering deploying remote application servers? If yes, are they capable of being boot servers?

  If you are planning on installing remote application servers for Domino or other applications, the same sort of considerations as mentioned previously, also apply here. For example, will you have TCP/IP and (preferably) OS/400 V4R2 or later installed on the remote AS/400? In addition, capacity needs for the IBM Network Station users should be considered. Will the users need to access AS/400 systems or other systems across the network. If so, is your network already TCP/IP capable?

- Does your organization have the necessary skills (either centrally or at the remote site) to install and maintain remote boot servers?

  Although the AS/400 system is well known for its ease of use and is ideally suited for use as a distributed system, consideration must be given to how the remote system will be installed and maintained. For example, do you have available skilled resource, either centrally or remotely located, to install the systems initially and provide ongoing support? Although a near *lights out* operational environment in your remote sites can be achieved, skilled resources at your central site will be required. In addition, outside help from sources like IBM Global Services or IBM Business Partners is also available to provide assistance during initial installation or ongoing maintenance.

- Is your network already TCP/IP?

  If your network is already TCP/IP capable, much of the necessary initial TCP/IP planning has already been accomplished. However, it may be that your central site is SNA only, but your remote site system is using TCP/IP so that IBM Network Stations can be used. If your users at the remote site are using applications located *only* on the remote system, then one key consideration is how to best facilitate central help desk personnel in supporting these new remote IBM Network Station users. For example, in the case where the centralized help desk is on an SNA only network, a centralized help desk person does not have the ability to directly telnet into the remote AS/400 system or into the IBM Network Station’s User

Services Console log. As an alternative, Display Station Passthru can be used to sign on to the remote AS/400 system and then a native AS/400 Telnet session can be used to *view* the Network Station User Services Console.

An example of a remote boot server environment is shown in Figure 5. In this scenario, the TCP/IP network is comprised of a central site AS/400 in Chicago, two remote sites with AS/400s and a mixture of PCs and IBM Network Stations. The central site in Chicago and the remote site in Boston are connected through routers across a wide area network. However, a PPP (point-point protocol) is used to connect the Seattle AS/400 system to the central site AS/400 system and network in Chicago. (PPP requires OS/400 V4R3 and V4R2 or later allows the AS/400 system to provide routing functions.) For the Seattle AS/400 system to provide routing functions for the other devices on its network, its TCP attributes had to be changed using the Change TCP/IP Attributes (CHGTCPA) command and specifying *YES for the *IP Datagram Forwarding* parameter.

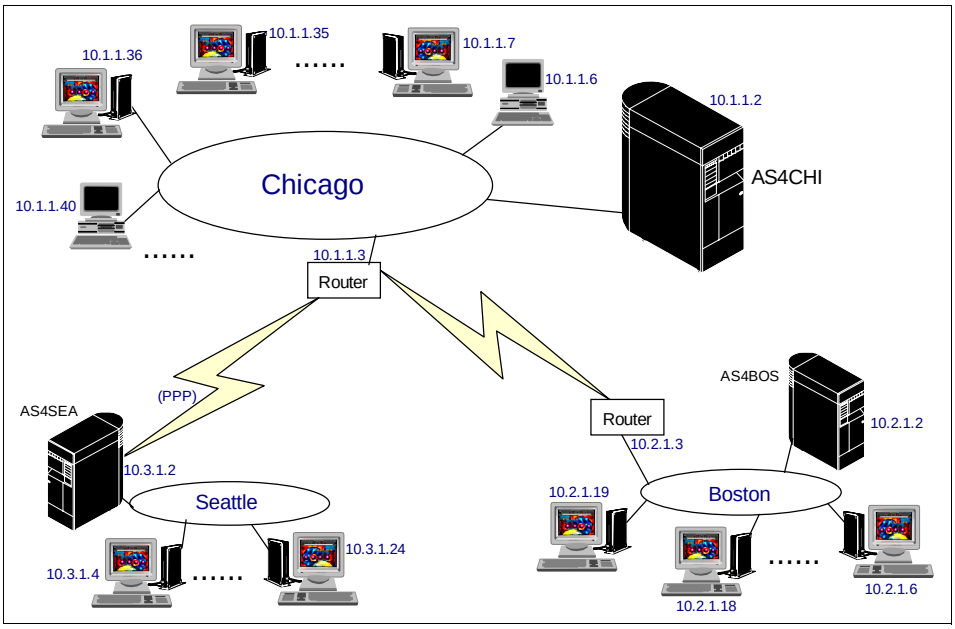


Figure 5. Remote Boot Servers Example

Please refer to Chapter 4, “Remote Servers and Split Boot Servers” on page 107 for additional information on the remote boot server option.

1.4.2 IBM 2212 Nways Access Utility

The new IBM 2212 Access Utility which was announced on September 22, 1998, is a multi-services networking device that provides more versatility, integrated functions and performance than a fixed function router or remote access server. This product offers the *combined* functions of a router, remote access server, Virtual Private Network Server and boot server in a cost effective, single box solution. The planned general availability for the IBM 2212 Access Utility was November 13, 1998. The IBM 2212 Access Utility is supported by the IBM Access Integration Services (AIS) Version 3.2 which was built using the same solid software base used by the IBM 2210 Nways Multiprotocol Router and IBM 2216 Nways Multiaccess Connector. The IBM 2212 and AIS V3.2 offer many features including:

- Comprehensive multiprotocol routing
- Security services
- Virtual Private Network (VPN) support
- *Integrated boot server* support for IBM Network Stations
- Up to 9 autosensing 10/100 Mbps Ethernet or 16Mbps Token Ring ports
- Up to 20 WAN ports supporting Frame Relay, ISDN, PPP, X.25, leased lines, channelized T1/E1 and X.25
- ISDN Basic Rate and Primary Rate interface

Given the purpose of this redbook, the most significant feature of the IBM 2212 Access Utility is its fully integrated *Thin Server Feature* which provides boot server support for IBM Network Stations. Using the IBM 2212 Access Utility as both a router for Internet and intranet access, as well as a local boot server can provide you with more efficient service to the IBM Network Stations and cost savings over the purchase of two separate devices. The IBM 2212 Access Utility is particularly well suited for the AS/400 environment for use at both central and remote sites because of its combined functions. In addition to providing Internet and intranet access and acting as a boot server, other 2212 Access Utility functions include IP routing, VPN support and comprehensive SNA and APPN features.

The IBM 2212 Access Utility is modular in design and comes in two standard model offerings, the model 40F or 40H. The Model 40H is recommended when using the *Thin Server Feature* (TSF) because it comes with a standard 3.2GB hard disk and is pre-loaded with the Enterprise software package which includes the Thin Server feature. The Thin Server Feature of the IBM 2212 Access Utility allows IBM Network Stations to obtain most of its boot code from the IBM 2212 Access Utility and only a small amount of data needs transporting across the wide area network infrastructure.

A major advantage of this remote site solution is that there is minimal setup and maintenance required in comparison to the remote boot server option. In addition, unlike the Flash boot option, the boot files located on the IBM 2212 are *automatically updated* when necessary. Also, keep in mind that this device provides router and remote access functions, as well as the boot server function. However, we recommend that no more than thirty IBM Network Stations be active at one time. Alternatively, an appropriately sized remote AS/400 boot server using the subnet broadcast boot can handle significantly more than thirty IBM Network Stations.

An example showing the use of the IBM 2212 Access Utility is shown in Figure 6. In this example scenario, the central site AS/400 system in San Diego already has a number of IBM Network Stations booting from it, as well as attached personal pomputers. In addition, a new remote branch in Raleigh is opened and the IBM 2212 Access Utility Model 40H and its Thin Server Feature is used to boot the attached IBM Network Stations at the remote site. These IBM Network Station users can then use 5250 emulation to access the central site AS/400 system as well as any of the other native IBM Network Station applications like 3270, VTxxx emulation or the NC Navigator browser.

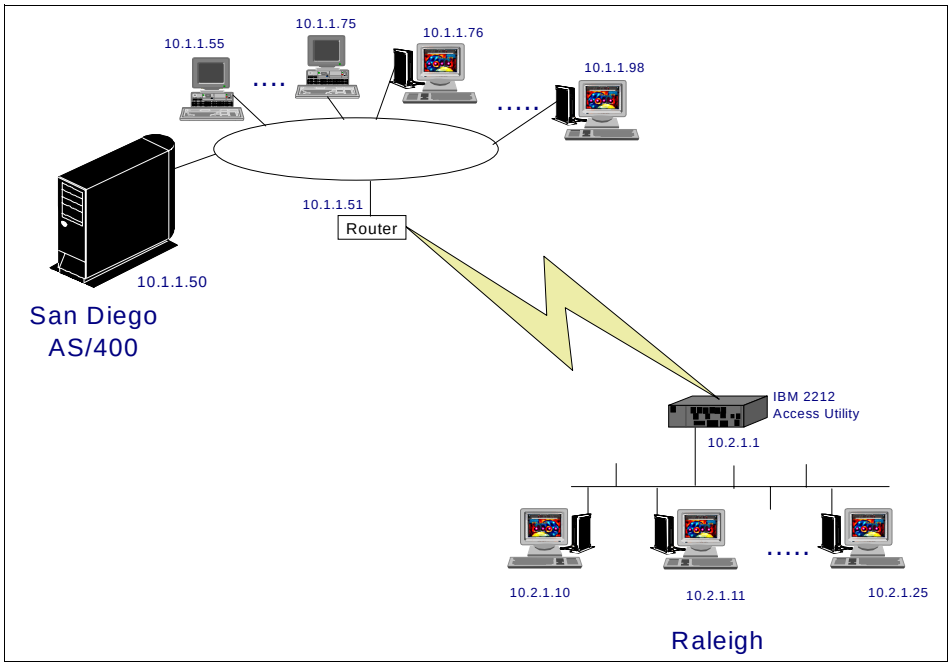


Figure 6. IBM 2212 Access Utility

For additional information about planning for, and implementing the IBM 2212 and the Thin Server Feature, refer to the manuals: *IBM 2212 Access Utility Introduction and Planning Guide*, GA27-4215, and *IBM 2212 Access Utility Installation and Initial Configuration Guide*, GA27-4216. These manuals are available online at the Web site: www.networking.ibm.com/did/2212bks.html

In addition, as mentioned previously, a future IBM redbook discussing the IBM 2212 Access Utility is planned for availability in 1999.

1.4.3 Flash Memory Card Boot

Another option available to you for small remote sites is to use local Flash Memory Cards. The Flash Memory Card enhancement for IBM Network Station Manager, Release 3, allows you to store the IBM Network Station operating system and applications on certain third-party Series D Type II PCMCIA memory cards and boot a remote IBM Network Station locally. Linear Series C cards are also supported but these are limited in size to 10MB, whereas the Series D cards are available in a range of sizes up to 32 MB and in the near future will most likely support 40MB.

IBM has tested PCMCIA memory cards from both Centennial Technologies and Simple Technology. After you obtain a new Flash card, it must first be formatted and then files can be copied to it. The IBM Network Station's NVRAM is then changed to indicate that the Network Station is to boot itself from this local media. Details on this procedure are discussed in Section 3.3.10.2, “Modifying the NVRAM Configuration for Local Boot” on page 91.

In addition to the (mandatory) operating system, the code to be booted can include any of the optional software modules for the IBM Network Station such as emulators, browser, ICA client, window manager, JVM, and fonts. In addition, the Flash card may contain user Java applications. One of the first steps is to determine which files you want to place on the card and what size Flash memory card you will need. Also, consider that separate files are sometimes required for the Series 1000 models. Therefore, if you intend to peer boot a mixture of Series 1000 and other models, you will need both sets of files and the card size approximately doubles. We highly recommend you place larger, more stable files on the card and let other smaller files, such as configuration preference files, download from the server across the network.

The local Flash card and *peer boot* solution is normally less expensive than the other solutions. However, a maximum of 10 IBM Network Stations booting from a peer IBM Network Station have been tested by IBM. In addition, after selecting the files to put on the card, you must *manually* maintain the Flash

cards because there is currently no automated way of keeping the files on the Flash card and the server synchronized.

For ordering and other information about obtaining Flash memory cards, software, and documentation necessary to use this functional enhancement, please contact your IBM representative or an IBM Business Partner and refer to PRPQ P97000, 5799-GEB, Feature Number 4002. In addition, unless you have one of the few early Ethernet IBM Network Stations which shipped with a PCMCIA slot, you must purchase a PCMCIA Adapter option for your Series 1000. This chargeable PCMCIA Adapter (part number 07L8336) option can be ordered by contacting your IBM representative or an IBM Business Partner. Additional details on the PCMCIA Adapter option and using Flash memory cards can be found online at the Web site:
www.pc.ibm.com/networkstation/solutions/product.html

Note

If a *boot server capable* system exists in your remote sites, give careful consideration to using it rather than a Flash card solution due to the non-automated maintenance nature of Flash cards.

A peer boot scenario in which Flash memory cards are used is shown in Figure 7 on page 30. As shown, the central location consists of an AS/400, S/390 and RISC/6000 systems, which are connected to a remote location across a wide area network link. In this case, one of the remote IBM Network Stations has a Flash memory card inserted into it which contains the operating system kernel and the executable modules required for the native 5250, 3270 and VTxxx emulators. This Flash card is used to boot the Network Station it is inserted in and any other Network Stations at the remote site on that subnet. However, after user authentication is done by the central site AS/400, user preferences, fonts and other more volatile data is downloaded from the central site. Please refer to Chapter 3, “Using Flash Cards with the Network Station” on page 63 for a comprehensive discussion of Flash card scenarios.

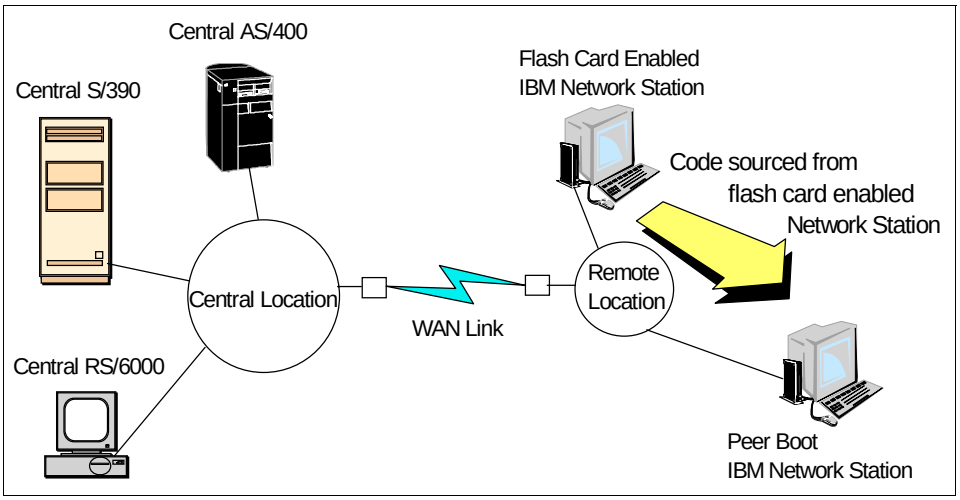


Figure 7. Remote Site - Flash Memory Card Peer Boot Example

1.4.4 Network Station Terminology

The following are definitions of terms that are used throughout this redbook.

Kernel (or operating system)

Both terms are used to refer to the IBM Network Station operating system which consists of a small, multi-tasking, UNIX-derivative kernel. It provides X Window support and also recognizes a limited set of commands to run built-in applications. Numerous extensions and libraries provide modular functionality for emulators, browser, console, ICA client, and so on.

Flash memory cards

PCMCIA cards which normally vary in memory capacity sizes from 8MB to 32 MB (or 40MB in the near future). These cards can be loaded with the IBM Network Station operating system kernel, files, and applications. They are also often referred to as Flash, Flash memory or Flash card.

Flash boot (or Flash memory boot)

Normally used interchangeably to refer to the process of loading an IBM Network Station from a PCMCIA Flash memory card.

Peer boot

Process through which an IBM Network Station containing a loaded Flash memory card can be used to boot other IBM Network Stations on its own subnet network.

Split boot

Refers to the use of the Release 3 separation of servers function to split or separate functions that occur during the boot up or initialization of the IBM Network Station. For example, an IBM Network Station could obtain its operating system kernel from a base code server and obtain other files, preferences and applications from another boot server.

Chapter 2. Planning Considerations

In this chapter, we discusss the planning considerations for implementing Network Stations in the AS/400 environment. Implementing Network Stations can vary from very simple transitions from non-programmable terminals (NPTs) to network stations with emulation only, to very complex installations where combinations of NPTs and PCs are migrated to a full function browser and collaborative environment. Some of the topics we discuss must be considered for both implementations. Our approach is to ask some basic questions that you need to answer to fully document your implementation plan.

2.1 Where You Are Currently

This first question is important: *Where are we now?* Whether you are the technical project planner for a multi-national corporation, or the part-time I/T support specialist on contract to a small business, you need to ask the following questions:

Current Host Applications (5250, 3270)
What are my current host application?

Define the access requirements that you are currently providing to your end-users. This helps you plan the desktops on the Network Stations and the systems to which they will be connected.

Service Levels for these Applications
Do service level agreements exist in your organization?

While you may not have formal arrangements with the end-user departments you are supporting, but there are implied agreements. For example, the users expect that the system is always up by 8:00am and available until 7:00pm. When an end-user powers on a terminal, the sign-on display appears almost instantly. Existing PC users also have expectations. For example, it takes 20 seconds to boot up Lotus 123 or AmiPro, and file saving is almost instantaneous.

These end-user expectations must be reset when you embark on your project to implement Network Stations to replace NPTs and existing PCs. The following are areas of systems management that must be reviewed as part of your implementation planning:

- Availability
- Performance

© Copyright IBM Corp. 1999

- Security
- Capacity
- Operations
- Problem
- Change Management

Communications Network
How much capacity do you have within your network?

Do you need to increase the capacity to support current and future requirements of your end-uses ? These items require some detailed investigation to accurately size the network.

Resource Availability
Are there resources available to support this project?

There is a requirement for skills in networking, host systems, PCs, project management, system and network sizing. There is also a need for training of the IT department and end-users.

Future Enhancements
Are there any enhancements required to meet the needs of the business?

Any enhancements should be carefully planned and aligned to defined business needs. Implementing browser-based or server-based applications is a complex environment unless you have skilled resources. Consider replacing the access to an existing application before moving to the a more complex environment. Then, move to the new environment in phases. This allows you to analyze the impact on the network and servers without jeopardizing the service levels of your existing services.

After you have answered the questions, and documented them, you can now move forward and ask more questions: *What are we trying to achieve? How are we going to get there?*

The answer to these questions are driven by the business units. However, not all the answers are known. There will be a number of iterations of the project plan before you get something workable. This may seem a large and extensive piece of work, especially if a project of this size has not been done before. You will not regret this investment of time later in the project. By installing Network Stations, you open your NPT users to the world of personal computing and the Web. You provide access to leading edge applications, collaboration and stability.

2.2 What You Are Likely to Have Now

Figure 8 shows examples of network components that may exist in your organization. We detailed as many example connections as possible (hopefully not all these examples exist at one time).

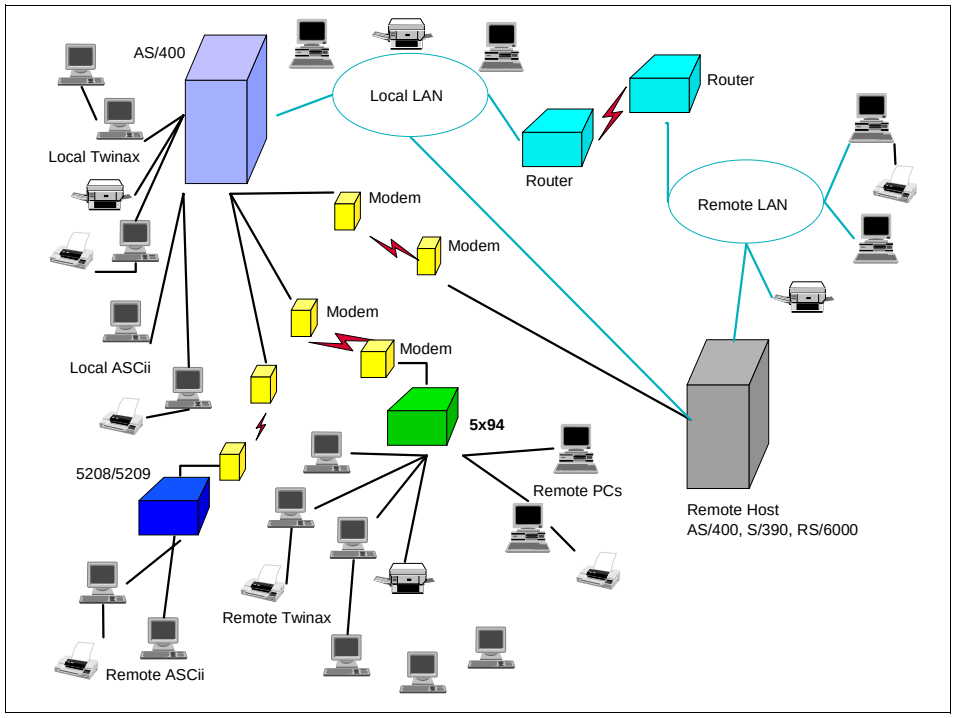


Figure 8. Network Components that May Exist in Your Organization

As shown in the example, there are more complex network components, such as LAN Bridge and Host-to-Host. These types of connection require a higher level of networking knowledge. However, the planning and installation concepts are similar to those found in Network Station implementation.

2.3 What You Are Trying to Achieve

The following diagram shows some types of connections you can make with a Network Station. There is overlap in the methods used. You may not use all of them.

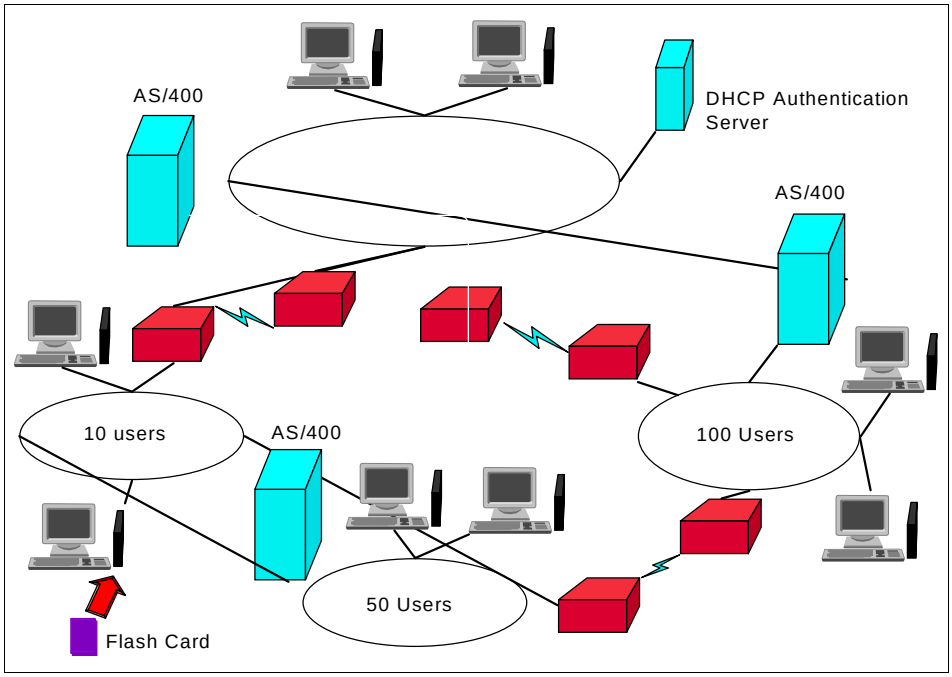


Figure 9. Network Station Implementation

The best place to start the discussion on these options is at the bottom of Figure 9. In this scenario, there are 50 users in a stand-alone organization, which has it's own I/T function. This is the simplest setup and easiest to compare with an existing NPT network. All information is stored on the local AS/400 system. Users have sign on capability to all other AS/400 systems in the network. Maintenance of these users is performed locally. Customizing is done in NVRAM, as the users are in easy reach of the IT function. However, depending on how frequently user requirements or application access change,s it is better to control configurations centrally. Plan this as though it were a system replacement. Performance must be considered if the AS/400system is particularly small. If you are replacing workstations with twinax attached network stations, do not use broadcast boot.

In the next scenario, there is a small group of 10 users attached to a central system with no local server capability. This is an example of a potential Flash card implementation. There are no local servers to hold boot information and the number of users is small. Provided the users do not have huge Flash memory requirements, Flash boot is a good choice. Ensure a duplicate Flash card is sent to the site to reduce the impact of a primary card failure. If Flash boot is not an option, consider the line speed and the installation of a local

boot server. A small AS/400 system is a very cost effective solution in comparison with a local PC server. This system can be managed very effectively from the central site.

If you look at the 100 users group, there is a local server that can provide boot information. You do not want to impact its work load. In this scenario, you can use Broadcast boot. This provides faster bootup, and central management, or again, you can could implement a small AS/400 system to act as the boot server.

If you look at the entire diagram as one organization, you can combine all three methods, depending on your management policies. Management from the central site is a good solution and this can be achieved very simply. If there are good AS/400 system, TCP/IP skills, it is possible to introduce a DCHP server to allow roaming and control the IP addresses (see Chapter 4, “Remote Servers and Split Boot Servers” on page 107).

2.4 Capacity

When investigating capacity requirements, consider the capacity of the network, and the utilization of the servers. If the network is old and has limited capacity, plan to upgrade. When the users realize the functionality delivered by the Network Station, demands on the network will grow tremendously, possibly overloading the available bandwidth. The network must be able to cope with the availability demands of the organization. Backup routes must be available if one link goes down. A network capacity study is time well spent. Any network with a mixture of systems and PCs may have a considerable latent demand.

The servers in the network must have the capacity to support the line of business applications and the CPU power needed to start up the users during normal logon and restart after failure. If broadcast boot is an option, then this reduces the demand on the server. If logon time is critical, consider installing local boot servers, especially where the network is one of the limiting factors.

Capacity is a very diverse topic and depends on the particular organizational requirements.

2.5 Performance

Performance information for Releases 1 through 3 for Network Stations attached to an AS/400 V3R2, V3R7, V4R1 and V4R2 is described in this

section. The following Network Station functions are included in the discussion:

- Time to initialize the Network Station (prior to login) for Ethernet, Token-Ring and twinax
- Time to load the applications (5250 emulation, browser, and so on)
- 5250 application performance
- Browser performance
- Java Virtual Machine (JVM) applet or application performance
- Times for the Network Station Series 100, 300 and 1000

The computer industry has a generic name for the IBM Network Station - the *thin client*. Because clients attach to servers, it may seem that an AS/400 server model attached to a Network Station (a thin client) would always be the best fit (that is, client-to-server). Be cautious when the Network Station is attached to an AS/400 server model as contrasted to a traditional system model. When using 5250 applications, the Network Station looks like a non-programmable terminal (NPT) (such as an interactive job) to the server and is subject to the AS/400 server interactive rules. Therefore, it may not always be a good choice. The traditional AS/400 system models with the Network Station are always a good choice.

2.5.1 Network Station Network Data

Table 2 on page 39 shows the amount of data that flows from the AS/400 system to each Network Station for initialization and each application load.

Table 2. Elements Loaded to a Network Station (MB)

Release	Release 1-2.5		Rel 3	Rel 3 DBCS*
Series	**100/300**	**1000**	**All**	**All**
Kernel+Configuration +other	4.0	4.8	3.0	3.9
5250 Emulation	0.9	0.9	1.6	3.8
3270 Emulation	0.3	0.3	0.9	3.2
IBM Network Station Browser	2.2	2.2	NA	NA
Navio NC Navigator	3.7	3.7	5.0	10.00
Java Virtual Machine	1.5 - 5.0	1.5 - 5.0	1.5 - 5.0	1.5 - 5.0
Note: *DBCS support includes Korean, simplified Chinese and Traditional Chinese				

Note

The amount of data downloaded may vary, depending on the configuration selected.

The kernel or configuration data is downloaded when the Network Station is powered-on. Unless configured otherwise, all other options are downloaded when they are selected.

When an application (for example, 5250 emulation) is closed or the user logs out, that application is downloaded again when it is next selected because it is not kept in memory across log-outs. The kernel or configuration data is kept in the Network Station across log-outs.

The download data for the Java Virtual Machine varies, depending on the application. Only the required classes are downloaded.

In Release 3, some of the information that is sent to the Network Station is compressed. The Network Station decompresses it after it is received. This compression means fewer bits are shipped from the AS/400 system to the Network Station, which results in better LAN utilization. More data and function is shipped to the Network Station in Release 3 than in previous releases. However, the compression results in boot performance that is about equal to previous releases.

Release 3 contains an option, *TFTP subnet broadcast*, that can significantly decrease the amount of data transmitted during the boot process, as well as saving significant CPU cycles in the AS/400 system. This option is described in more detail in the following sections.

2.5.1.1 IBM Network Station Initialization

Initialization, at this time, is non-trivial and can be a performance concern for some customers. The time required to initialize the Network Station, particularly when many Network Stations are initialized simultaneously, can be prohibitive. In addition, initialization can consume a lot of AS/400 CPU useage, which may impact other jobs on the AS/400 system.

If possible, it is best to leave the Network Station powered-on after initialization or to stagger initialization. The IBM Network Station consumes very little power. If initialization times are a problem and power outages are a concern, consider battery backups for each IBM Network Station, or server systems dedicated to initialization.

2.5.1.2 Initialization Mechanisms

Initialization is performed using TCP/IP Trivial File Transfer Protocol (TFTP) and AS/400 Remote File System (RFS). Both of these access methods read files from the AS/400system to the Network Station. For reliability and performance, both mechanisms subdivide files into blocks for sending, and then recombine them in the Network Station. The TFTP block size can be configured as 512 to 8192 bytes. The RFS block size is currently fixed at 8192. TFTP and RFS is used during initialization depending on the configured initialization options.

There are three possible ways to initialize the Network Station:

- **NVRAM**

  The AS/400 system and Network Station IP addresses and other information are configured in each Network Station. The Network Station sends a TFTP request to the configured server to begin initialization.

- **BOOTP**

  The Network Station broadcasts to find a responding AS/400 server. The AS/400 server is previously configured with the IP address and other information for each Network Station . After the server receives a broadcast from a Network Station, it begins the initialization.

- **DHCP**

  The same as BOOTP except the AS/400 server contains a pool of Network Station IP addresses. BOOTP or DHCP is the preferred method, for

Releases 1 though 2.5. All methods are suitable in Release 3. For Releases 1 though 2.5, NVRAM uses TFTP to load the kernel/configuration files and, after login, uses RFS. For Release 3, NVRAM uses TFTP to load the kernel and RFS for all subsequent files. BOOTP and DHCP use TFTP to load the kernel and then use RFS to load all subsequent files.

For Releases 1 though 2.5, the Network Station tries 10 times, with a five second timeout, to locate and read the kernel using TFTP. After 10 attempts, an error message is sent. For Release 3, the Network Station can be configured to try indefinitely to locate and read the kernel.

For Releases 1 though 2.5, if NVRAM is selected, the Network Station reads the configuration files using TFTP. The Network Station tries 10 times, with a three second timeout, to read each file. If unsuccessful, it skips that file and then tries to read the next file, which eventually results in an unsuccessful initialization. RFS has an infinite retry and does not skip files. From a reliability perspective, this makes NVRAM, for Releases 1 though 2.5, the least preferred booting mechanism.

With Network Station Manager Release 3, subnet broadcast is available over Ethernet, token-ring, and twinax. When this option is selected, TFTP data (for example, the kernel is about 2MB), is broadcast from the AS/400 server to any requesting Network Station.That is, the kernel is sent one time so that each Network Station receives it. When subnet broadcast is off, the kernel is sent individually to each Network Station, which means a lot more data on the LAN or twinax. The broadcast is only to a subnet (such as any Network Station on a single ring, such as 9.5.112.x).

When Network Stations from different subnets request the kernel, the AS/400 server provides a broadcast to each subnet. The data below shows that subnet broadcast uses less AS/400 CPU. Subnet broadcast is the preferred boot option (twinax has some special considerations discussed later). There is a caution, some routers do not support broadcast and broadcast can cause other problems, if not configured properly.

Subnet broadcast is supported on twinax. Unlike Ethernet and token-ring protocols, the twinax protocol does not support broadcast. What this means for twinax, is that, when subnet broadcast is selected, each frame is sent individually to each device. When all devices are expecting the broadcast, this option works well (less AS/400 CPU). When all devices are not expecting the broadcast, this option results in more data on the twinax cable. The following information shows this. *In general, customers should not use subnet broadcast for twinax.*

Some customers who have Series 1000s have experienced performance problems. The Series 1000 supports both full duplex and half duplex. In general, the performance problem is caused by a configuration error. As a result, the Series 1000 tries to operate in full duplex mode, but a router or something else in the network supports only half duplex. The Series 1000 almost continuously runs into collisions on the Ethernet, which results in extremely slow performance.

Some customers, who have Token-Ring network switches that pass 4K frames, have experienced difficulties. These customers set their LAN frame size or MTU to a value greater than 8K. In general, these customers used NVRAM, with a default 1024 TFTP block size. Initialization works fine until login, when RFS takes over and uses 8K frames. The 8K frames do not pass through a 4K switch. Some solutions to this problem may be to configure the switch to allow 8K frames, replace the switch with a router, or configure the AS/400 LAN frame size/MTU to 4K (twinax is fixed at 4K).

If the network has no Domain Name Server (DNS), performance can be very slow, since DNS time-outs in the region of 30 seconds occur frequently. AS/400 V4R2 contains DNS support. If a customer does not wish to use a DNS, for Release 3, good performance is still possible by performing the following steps:

1. Enter CFGTCP. Select option 12 (*Change TCP/IP domain information*). Set *Search priority* to ***LOCAL**.
2. Enter CFGTCP. Select option 10 (*Work with TCP/IP host table entries*). Add the IP address and host name for the AS/400 system and each Network Station.
3. Using Network Station Manager, select **Hardware —> Workstations —> Domain Name Server**. Set *Update Network Station Manager DNS file.*

The initialization options described in this redbook is adequate for most customer environments. There are other variations that can occur. For example, if the customer chooses BOOTP and successfully loads the kernel, but, for some reason, RFS is not working properly, initialization times out on RFS and switches back to TFTP. Variations, such as these are not described in this document. The BOOTP boot sequence is described in greater detail in the following section.

2.5.1.3 BOOTP Initialization

There are four steps in the BOOTP initialization process. To get a total initialization time, you need to add together the times from each.

1. Hardware test

The hardware test is just that, a memory test and other hardware tests to insure that the Network Station hardware is operational. For the most part, the length of this test is determined by the amount of memory in the IBM Network Station.

Table 3. Time (Seconds) to Perform Hardware Test

Memory (MB)	Series 100	Series 300	Series 1000
8	15	14	-
16	18	18	-
32	24	22	10
48	30	26	-
64	36	31	13

2. Kernel or configuration initialization

   In this step, the Network Station locates the AS/400 server, reads the kernel and configuration files, and then displays the login window.

   The Network Station broadcasts a BOOTP request to locate the AS/400 server and then the kernel (about 2MB) is read using the TFTP function of TCP/IP. The configuration files are then read using the Remote File System (RFS). The time to load the kernel using TFTP is heavily dependent on:

   - TFTP block size
   - TCP/IP maximum transmission unit (MTU) size
   - LAN line description frame size
   - TFTP subnet broadcast option number of TFTP jobs
   - Number of TFTP jobs

   The Network Station negotiates the TFTP block size with the AS/400 server. It can range from 512 to 8192 bytes. The Network Station default is 8192. In general, the Network Station uses the TFTP block size, MTU and frame size defined by the AS/400 server.

   The AS/400 server default TFTP block size is 1024. As shown in the following tables, best performance is obtained with a large TFTP block size (such as 8192). If the MTU or frame size is less than 8192 (Ethernet has a maximum frame size of 1492) performance, can be enhanced by configuring the block size greater than the MTU or frame size. If the TFTP block size is greater than the MTU or frame size, TCP/IP fragments (subdivides) the TFTP blocks to fit into the MTU or frame size. The Network Station TCP/IP recombines the MTU or frames into TFTP blocks. This fragmentation provides better performance than setting the TFTP

block size equal to the MTU or frame size. Users must be aware that some routers, switches and gateways do not support this fragmentation capability. Twinax MTU or frame size are fixed. Therefore, fragmentation does not apply to twinax attached Network Stations.

The number of TFTP jobs on the AS/400 server is also a performance factor. The optimal number, for a system with a single LAN IOP, is about six (the default). The TFTP jobs are a pool of AS/400 jobs that download the kernel to Network Stations. They are on a f*irst come, first serve* basis. If there are more Network Station requests than jobs, the excess is ignored (not queued). If a request is not satisfied, the Network Station repeats its request, every five seconds. In general, there should be six TFTP jobs for each LAN IOP that has attached Network Stations.

The following tables and figures show how the TFTP block size affects the kernel and configuration initialization time, for a few AS/400 system sizes. The tables also show what happens when 1, 10, 50, and 100 Network Stations simultaneously (such as, after a power outage) request TFTP initialization. The times represent the number of seconds when the last Network Station completes its TFTP and RFS download. The data in the following tables was obtained in a dedicated environment. That is, only BOOTP, TFTP and RFS were running on the AS/400 server and there was no other load on the LAN. In each test case, the base pool was cleared before beginning the test.

Important

Results listed here do not represent any particular customer environment. Actual performance may vary significantly from what is provided here.

Each of the following runs had the following configured:

- 8K Maximum Transmission Unit (MTU)
- 8K Frame Size
- 6 TFTP jobs

Table 4. Kernel/Configuration Initialization Time

AS/400 Model F97 (V3R2) IBM Network Station Series 300 Release 1-2.5 16Mb token-ring Vary TFTP Block Size					
#NS	**512**	**1024**	**2048**	**4096**	**8192**
1	109 (5.0)	46 (5.5)	34 (4.2)	29 (2.9)	26 (2.6)
10	225 (27.0	105 (31.0)	77 (26.0)	63 (22.6)	57 (12.2)
50	992 (32.8)	470 (41.7)	327 (30.8)	257 (24.0)	209 (20.1)
100	1885 (35.2)	890 (46.3)	624 (33.6)	503 (25.5)	395 (22.3)
Note: Time in seconds (Average CPU in %)					

Table 5. Kernel/Configuration Initialization Time

AS/400 Model 150-2270 (V3R7) IBM Network Station Series 300 Release 1-2.5 16Mb token-ring MFIOP Vary TFTP Block Size					
#NS	**512**	**1024**	**2048**	**4096**	**8192**
1	85 (23.3)	35 (28.6)	31 (22.0)	27 (16.3)	26 (14.8)
10	229 (87.8	126 (82.2)	83 (72.9)	63 (63.4)	55 (53.6)
50	1065(94.2)	565 (95.0)	347 (92.0)	234 (87.6)	193 (77.6)
100	2075 (97.5)	1119 (97.0)	682 (94.5)	448 (92.5)	352 (88.1)
Note: Time in seconds (Average CPU in %)					

Table 6. Kernel/Configuration Initialization Time

AS/400 Model 510-2144 (V3R7) IBM Network Station Series 300 Release 1-2.5 2619 16Mb token-ring IOP Vary TFTP Block Size					
#NS	**512**	**1024**	**2048**	**4096**	**8192**
1	71 (9.8)	59 (7.4)	52 (6.4)	46 (5.8)	43 (5.2)
10	169 (39.3)	117 (30.3)	81 (26.1)	65 (21.2)	62 (17.3)
50	790 (44.5)	451 (42.5)	361(32.6)	265 (28.7)	209 (27.0)
100	1526 (47.3)	875 (45.2)	667 (35.7)	498 (31.7)	384 (30.5)
Note: Time in seconds (Average CPU in %)					

Table 7. Kernel/Configuration Initialization Time

AS/400 Model S30-2257 (V4R1} IBM Network Station Series 300 Release 1-2.5 2629 1 6Mb token-ring LAN IOP Vary TFTP Block Size					
#NS	**512**	**1024**	**2048**	**4096**	**8192**
1	96 (1.8)	41 (4.3)	33 (4.5)	30 (3.7)	29 (3.6)
10	182 (14.4)	73 (16.4)	56 (12.7)	52 (8.9)	39 (8.5)
50	735 (18.9)	279 (24.9)	201 (20.2)	146 (17.5)	127 (15.3)
100	1382 (20.2)	513 (27.7)	357 (23.2)	272 (20.0)	244 (16.6)
Note: Time in seconds (Average CPU in %)					

Table 8. Kernel/Configuration Initialization Time

AS/400 Model 400-2132 IBM Network Station Series 300 Release 1-2.5 2629 10MB Ethernet LAN IOP Vary TFTP Block Size					
#NS	**512**	**1024**	**2048**	**4096**	**8192**
1	76 (35.6)	53 (26.3)	45 (19.8)	39 (17.7)	34 (15.5)
10	280 (90.2)	167 (82.0)	110 (72.6)	83 (63.7)	67 (55.7)
50	1311 (97.5)	745 (93.8)	467 (88.6)	321 (82.1)	277 (69.3)
100	2691 (97.82)	1466 (96.9)	895 (93.4)	623 (86.7)	540 (73.1)
Note: Time in seconds (Average CPU in %)					

Table 9. Kernel/Configuration Initialization Time

AS/400 Model 400-2132 (V4R1) IBM Network Station Series 300 Release 3 All NSs attached to a single twinax adapter Vary twinax Adapter type, subnet broadcast and TFTP block size Vary Twinax					
#NS	**6050 without subnet 8K TFTP**	**6180 with subnet 1K TFTP**	**6180 without subnet 1K TFTP**	**6180 with subnet 8K TFTP**	**6180 without subnet 8K TFTP**
1	107 (8.5)	114 (22.0)	116 (22.1)	87 (14.5)	82 (13.3)
2	173	155	133	90	85
3	225	165	154	106	98
4	275	168	159	121	116
5	325	186	178	142	139
6	388	201	199	155	157
7	446 (16.4)	225 (33.6)	221 (70.0)	171 (28.8)	162 (37.5)
Note: Time in seconds (Average CPU in %)					

Note

Notice that subnet broadcast uses less AS/400 CPU. However, as discussed previously, each twinax device on the subnet gets their own copy of the broadcast data, even if they did not request it, which would mean unwanted data on the twinax cable. In general, you should not use twinax subnet broadcast. Subnet broadcast should be used on LANs.

In Table 9, the Network Stations are all chained to a single cable port. For the 6180 adapter, faster times can be obtained if the Network Stations are balanced across cable ports, with half on ports 0 through 3 and the other half on ports 4 through 7. For example, in Table 10 on page 49, six Network Stations with an 8K TFTP block size, without subnet broadcast, booted in 157 seconds. If they were balanced, three on port 0 and two on port 4, the initialization time would be 130 seconds or 17% faster.

If a Network Station has multiple paths, with the same network address, to an AS/400 (such as, two IOPs that each have a path to the Network Station), unexpected results can occur. Whenever the AS/400 server gets a request from a Network Station, it uses the default path to get back to the requesting Network Station. The return route (and any subsequent request or replies) can be different from the original request. This implies that there is no value to add a second IOP with the same network address to gain additional TFTP performance.

TFTP jobs are assigned on a first come, first serve basis. There is no mechanism to allocate a TFTP job to a particular IOP. This implies that it is possible for Network Stations attached to one network to monopolize all the TFTP jobs until completion of the kernel download. Other IBM Network Stations can starve until a TFTP job is available.

3. Login

   Login is just that, users enters their user ID and password and then the desktop appears.

   The load times can be found in the Table 10 on page 49.

4. Application Load

   Applications are loaded when their respective desktop buttons are selected. Load times vary by AS/400 machines size.

   Getting to a 5250 sign-on display can require two steps:

   a. From the menu bar, select the **5250** button to get to the host name window.

b. Enter the desired host name to get to the 5250 sign-on window. Most administrators use the Network Station Manager to configure for direct menu bar to 5250 sign-on.

5. Getting to the browser is a single step. From the menu bar, select the **Browse** button to get to the NC Navigator browser.

   Examples of load times can be found in the following tables.

Table 10. Load Times (Seconds)

AS/400 Models 150-2270 and S10-2144 (V3R7) IBM Network Station Series 100 and 300 Releases 1-2.5 2619 16MB Token-Ring LAN IOP				
Processor/NS Model	2270/100	2270/300	2144/100	2144/300
User ID/password to desktop	10	10	15	11
5250 select to host name	9	6	10	7
Host name to 5250 login	6	6	12	11
Browser select to browser	33	16	41	22

Table 11. Load Times (Seconds)

AS/400 Models 400-2132 (V4R2)) IBM Network Station Series 300 Releases 3 eSuite is IBM Network Station Series 1000 Release 3 Twinax or Ethernet Adapter				
	6050	6180	2629	2629 DBCS*
User ID/password to desktop	30	27	18	23
5250 select to host name	57	33	10	19
Host name to 5250 login	15	21	12	14
Browser select to browser	169	131	41	52
eSuite to eSuite	-	-	175	-
Note: * DBCS support includes Korean, simplified Chinese, and Traditional Chinese				

In this subnet broadcast example, assume 100 Series 300 Network Stations attached to an AS/400 V4R2 2132 using a single 10Mb Ethernet

segment. Assume the electricity on all 100 Networks Stations goes out and some time later it comes back on. Assume the Network Stations all have the same memory size (for example, 32MB) and identical monitors attached. It is possible for all 100 to be at the Login window in 280 seconds (less than five minutes). The 280 seconds comes from: 21 seconds for hardware test, 30 seconds to load the kernel, and 229 seconds to load configuration files.

2.5.1.4 AS/400 5250 Applications

The Network Station user should see 5250 applications almost exactly as they were on the NPT or PC terminals. However, the load on the AS/400 server may be different. Network Stations use the AS/400 TCP/IP TELNET path. TELNET consumes 27% more CPU time per transaction than an NPT attached to a local twinax for a typical commercial workload. This yields a 20% capacity reduction over a twinax attached NPT. For comparison, a Client/Access PC using 5250 over SNA, when using the same workload, consumes 10% more CPU time per transaction than a local twinax attached NPT.

The implication is that customers migrating from local twinax attached NPTs to LAN attached Network Stations will probably use more CPU to run the same 5250 applications. Customers migrating from LAN attached SNA Client/Access PCs will also probably use more CPU. Customers migrating from LAN attached TCP Client/Access PCs should need no additional CPU capacity to run their 5250 applications.

2.5.1.5 Browser

In general, the Series 100, 300 and 1000 all perform equally well. Their performance should be comparable to that seen on a PC.

It is important that either SOCKS or Proxy are configured, but not both. Poor performance is seen when both are used.

2.5.1.6 Java Virtual Machine Applets and Applications

Java is still evolving. As such, its use on a Network Station is also evolving. The Series 100 clearly should not be used for Java. The Series 300, while twice as fast as the 100, can be used for very limited Java applets. The Series 1000 is for Java; however, since Java has varied uses, customers are encouraged to test their Java applications on the Series 1000 before putting them into production.

2.5.1.7 The AS/400 as a Router

The AS/400 is a router (data passes though it) when twinax attached Network Stations send or receive data from the Internet or other servers. At this time, limited performance data is available. The following two tables show results when data is read from an NT server through an AS/400 system to a Network Station.

Table 12. Load times (Seconds)

AS/400 Model 400-2132 (V4R2) IBM Network Station Series 300 Release 3, using 10MB Ethernet to AS/400 300Mhz PC NT server using 16MB TR to AS/400 2628 LAN IOPs, 15MB of data. 8K TFTP block			
#NS	**Time (sec)**	**AS/400 Util (%)**	**AS/400 Throughput (KB/s)**
1	44	11.2	340.9
2	48	16.9	625.0
3	57	18.1	789.5
4	71	25.7	845.1
5	90	24.4	833.3
10	158	29.9	949.4
15	232	34.9	969.8

Table 13. LAN to Twinax Throughput

AS/400 Model 400-2132 (V4R2) IBM Network Station Series 300 Release 3, using Twinax to AS/400 300Mhz PC NT server using 16MB TR to AS/400 2629 LAN IOP, 6180 Twinax Adapter, 2MB of data. 8K TFTP block			
#NS	**Time (sec)**	**AS/400 Util (%)**	**AS/400 Throughput (KB/s)**
1	33	9.9	70.1
2	48	9.9	96.4
3	109	10.3	63.7
4	127	10.5	72.9
5	150	11.1	77.1
6	213	11.0	65.2

2.6 Performance Conclusions

The Network Station provides for an excellent working environment. In general, the Network Station 1000 performs better than the 300, which performs better than the 100. The following section discusses the performance of the Network Stations.

Initialization

This section provides the initialization time conclusions for the Network Servers:

- The Network Station Series 1000 initialization time is about the same as the 300, except for hardware test, where the 1000 is faster. The 300 is faster than the 100.
- If possible, consider a boot server for each ring or Ethernet.
- For Releases 1 though 2.5, use BOOTP or DHCP. Do not use NVRAM. Implementations using BOOTP and DHCP are faster and more reliable. For Release 3, all three initialization mechanisms are equal in reliability and performance. BOOTP is slightly (1to 2 seconds) faster than DHCP. However, NVRAM is less flexible than DCHP or BOOTP because the entering of IP addresses at the Network Station itself, is required.
- The time to initialize Network Stations depends on many variables, such as the size of AS/400 system, TFTP block size, number of attached IBM

Network Stations, LAN utilization, CPU utilization, and so on. I/T Technical Support Staff must evaluate each project to produce the optimum network design. We recommend that, when you are building Network Station solutions, you phase the customer projects to ensure the design meets expectations with no surprises.

- Initialization time varies from AS/400 model to AS/400 model. In general, the larger the model, the better the performance. On larger models, the bottleneck is the LAN IOP and, on smaller models, the bottleneck is CPU and LAN IOP. The 2629 LAN IOP provides better performance than the 2619.
- 10Mb Ethernet, 100Mb Ethernet and 16Mb token-ring are about equal in performance within this environment.
- During initialization, CPU utilization can be quite high, especially on the smaller AS/400 systems, which will impact other jobs. In addition, TFTP requires more CPU than RFS.
- Subnet broadcast can significantly reduce LAN traffic and AS/400 CPU utilization. Subnet broadcast is available with AS/400 V4R2 and Network Station Release 3. If possible, we highly recommend that subnet broadcast be used. In general, subnet broadcast is not advisable with twinax, except as discussed earlier.
- The network administer should configure TCP/IP, LAN frame size and TFTP block size for best performance. In general, the larger the size, the better the performance.
- For twinax, the 6180 adapter is significantly faster than the 6050. The 6180 is about equal to a 4Mb token-ring.
- Because TFTP selects the path to use, there is no value to add a second IOP, with the same network address, to a LAN to get better initialization performance. All Network Stations, from the same network, use the TFTP selected path.
- It is best to configure six TFTP jobs per LAN that has attached Network Stations. However, for systems that have multiple LANs, since there is no way, at this time, to dedicate a TFTP job to a particular LAN, initialization may not perform as well as desired.
- In general, V4R2 provides better performance than V4R1, which provides better performance than V3R7. V4R2 contains TCP/IP and IOP LAN enhancements. In some cases, customers will see substantial improvements in kernel/configuration initialization. In general, these improvements will be visible when a single Network Station is initialized with a small TFTP block size. V4R2 contains RFS enhancements.

- Release 3 boots about as fast as previous releases, even though more data and function are sent. Much of the data sent is compressed.
- Switches, routers and gateways can cause problems. Ensure your Network Administrator is involved in the implementation.
- For 6180 twinax attached Network Stations, best performance is obtained if all Express Datastream enabled devices are on the same cable, excluding older, non-Express capable devices.
- When Express devices are attached to a single workstation controller, best performance is obtained by load balancing those devices. That is, half the devices should be connected to cable ports 0 through 3, and the other half should be connected to ports 4 through 7.

5250 Application Performance on the AS/400 System
This section provides the 5250 application performance conclusions for the Network Servers:

- In general, the 100, 300 and 1000 all perform equally.
- Migrating from LAN attached SNA Client/Access PCs will probably use more CPU (about 17%) to run the same 5250 applications.
- LAN attached TCP/IP Client/Access PCs will use about the same CPU as IBM Network Stations when running the same 5250 applications.
- Local twinax attached NPTs to IBM Network Stations migration will probably use more CPU (about 27%) to run the same 5250 applications.

Browsers
This section provides the browser conclusions for the Network Servers:

- In general, the 100, 300 and 1000 all perform equally.
- Poor performance is obtained when both socks and proxy are configured. Only one should be used.
- Never use disk caching.

Java Virtual Machine
This section provides the Java Virtual Machine conclusions for the Network Servers:

- The Series 100 should not be used for Java.
- The Series 300 can be used for limited, lightweight Java.
- The Series 1000 is for Java; however, since Java hasn't fully matured and can be used for many, varied applications, customers should insure that their Java application and the 1000 are compatible.

AS/400 as a Router

Limited data is available. A model 400-2132 is able to route about 970kb/s from one LAN to another and about 75Kb/s from a LAN to twinax.

2.7 Problem and Change Management

At times, the Network Station operating system may stop unexpectedly with a *PANIC* error. One of two symptoms may appear:

- *PANIC* appears on your Network Station and a > cursor is shown.
- The display turns reverse video (mostly black) and a > cursor is presented.

To recover from such a condition, you can power off and on the Network Station or if the *PANIC* error persists can contact IBM support. There are problem determination tools, available within the Release 3 code of the Network Station, which an IBM support person can invoke for further problem determination of the *PANIC* condition.

2.8 Migration Considerations

If you are upgrading from the 5733A07 (R2.5) to the 5648C05 (R3.0) level of the IBM Network Station Manager licensed program, consider the following items:

- **New Boot Monitor Code:**

  The boot monitor code in Release 3 contains new functions. We recommended that you update the boot monitor code on each of your Network Stations. For instructions on how to update the Boot Monitor Code, refer to *IBM Network Station Manager Installation and Use*, SC41-0664.

- **NC Navigator:**

  The IBM Network Station Manager Release 3 licensed program (5648C05) does not support the IBM browser. When you install Release 3, the 40-bit NC Navigator automatically installs. The bookmarks that you used with your IBM browser will be migrated to the new NC Navigator. If your users were saving both Navio and IBM Network Station bookmarks, the Navio bookmarks are migrated and the IBM Network Station browser bookmarks are saved to a file. The save file can then be imported into the NC Navigator browser. The 128-bit browser (available in the US and Canada) can be installed after Release 3 is installed successfully. Refer to Chapter 7, “Replicating a Remote Boot Server Environment” on page 213 a known problem with NC Navigator bookmarks, after migrating to Release 3.

- **Configuration Information and User Data:**

  Information that has been entered through the IBM Network Station Manager is migrated. If the configuration files have been *manually* edited, you can obtain additional information on how to migrate your configuration by referring to the Advanced User Information at: http://www.ibm.com/nc/pubs

2.9 Roaming

With the availability of Release 3 of the IBM Network Station Manager, you can take advantage of Multiple Server Environments. The servers required for the Network Station are:

- BOOTP/DHCP Server
- Base Code Server
- Terminal Configuration Server
- Authentication Server

For example, a user may be accessing one system for the BOOTP, Base Code and Terminal Configuration Servers. When the Network Station Login display is presented, the user can click on the **ROAM** button to enter another system that has the Authentication server running.

Roaming can also be coupled with *load balancing.* For further information about load balancing, refer to *IBM Network Station Manager Installation and Use,* SG41-0664.

2.10 Slow Link Boot versus Flash Card Peer Boot

Release 3.0 IBM Network Station Manager has been enhanced to provide Flash memory card support. This function is available in U.S. English for IBM Network Stations connected to any of the IBM servers supported by Release 3.0.

Flash memory card support enables the use of a PCMCIA Flash memory card to boot the IBM Network Station. Because the IBM Network Station has no disk storage devices, all the software required to make it operational must be loaded from a server. In environments where there is no local server, transferring megabytes of code over a WAN (Wide Area Network) can take several minutes. To reduce the time needed to boot in these environments, the Network Station operating system and applications can be stored on a Flash memory card.

Peer boot is a new function that allows multiple IBM Network Stations to boot from a single Flash card located in a local Network Station. The performance of Network Stations utilizing peer boot is very acceptable. Up to ten Network Stations peer booting simultaneously from a single Flash card were tested with very good results.

Because of the current size limitations of the Flash cards, it is not possible to store all of the code required to start and operate the Network Station on a single card. The largest and most static files are placed on the Flash card such as the kernel and executable modules. User configuration data, fonts and other slightly more volatile files (files that may change periodically) are loaded from the central server. Using this split boot technique, the system administrator can maintain configuration files from a central location using the IBM Network Station Manager program.

The management of the data on a Flash card is time-consuming and is not yet automated. There are no tools provided to synchronize the files on the Flash card with those on the server or even to indicate when the files on the Flash card are down-level from some designated configuration. In fact, the files within the Flash card (local) file system, have no timestamps. Therefore, it is not easy to tell which version of each software module is on the card.

To update the card while it is in the Network Station, it must first be NFS-mounted to a server and then the new files copied (at two minutes per Mbyte) to the card. If the link goes down or the card fills up, the card could be left in a partially-updated state.The Network Station is unusable until a correctly-formatted card is obtained.

For this reason, when updates are required, we recommend that you send a new Flash card to the necessary sites. The obsolete cards can be returned, reformatted, and Flashed again at a central location. This makes the Flash card very similar to CDROM from the administrator's and user's perspective. This arrangement works well as long as the environment is rather static and frequent updates are not required.

2.11 CISC and RISC Co-existence

The IBM Network Station Manager license program for AS/400 V3R2M0 is 5648-B06. All AS/400 internal references to this product, however, are denoted as 5733-A06. This code runs on CISC AS/400 systems.

There are two different levels of the IBM Network Station Manager license program that can be installed on AS/400 systems running V3R7M0 and above. They are the 5648-BOM (5733-AOT in GO LICPGM) (R2.5) and the

5648-C05 (R3.0) products. It is important to remember that Network Stations booted from an R3.0 NSM server can assess a V3R2 CISC AS/400 through 5250 Emulation. However, any Network Stations booting from a V3R2 system does *not* have the R3.0 enhancements available (for example, roaming capability, DCHP support, separation of servers, and so on.) because NSM R2.5 (not R3.0) is supported on V3R2.

Customers running R2.5 should migrate to R3.0 for:

- Support
- Year 2000 certification
- New functions

R2.5 to R3.0 is a seamless migration.

2.12 Printing with Your IBM Network Station

The following sections discuss configuring printers when using the IBM Network Station.

2.12.1 Configuring Printers on an AS/400 System

You can configure printers for your Network Stations with the IBM Network Station Manager program unless the datastream generated by the Network Station application does not match a datastream that your printer understands. Figure 10 on page 59 describes which datastreams the common Network Station applications produce. If your Network Station application does not produce a datastream that your printer understands, you must send the print job to an AS/400 server. The AS/400 server transforms the print job into the datastream of your choice.

Note

Transforming print jobs requires OS/400 Version 4 Release 2 or later. For example, if Network Station A in Figure 10 on page 59 generates a print job from NC Navigator for Printer 1 (a Printer Control Language (PCL) printer), the Network Station cannot send its print job directly to the printer. Because NC Navigator can only generate PostScript (PS) datastreams, the Network Station must send its print job to the AS/400 server, which will transform the print job into a PCL datastream. A queue on the AS/400 server then sends the transformed print job to Printer 1.

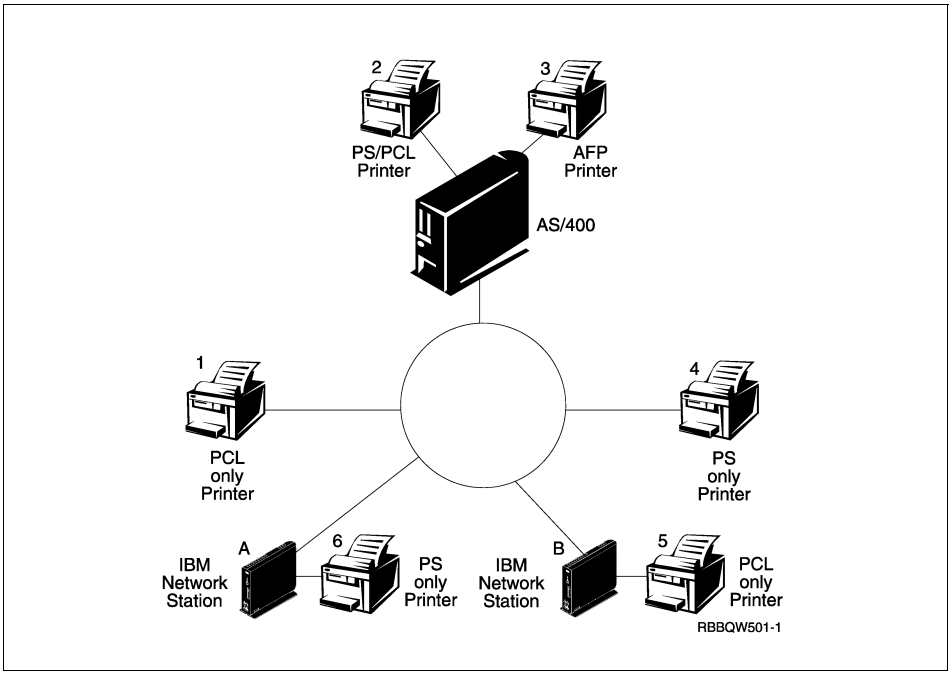


Figure 10. Possible Network Station Printing Scenarios

For server-based applications, such as a 5250 application, you must configure a printer on the server where the application is running. In this case, think of the Network Station as only a window to the server, in that server still performs the work. In Figure 10, if Network Station A runs a 5250 session on the AS/400 server and you want to print to Printer 4, you must create a printer device description on the AS/400 server. The AS/400 server sends the print job to Printer 4. To create a printing device description on your AS/400 system, use the Create Printer Device (CRTDEVPRT) command.

For a comprehensive printing information, refer to the *IBM Network Station Printing Guide*, SG24-5212.

2.12.2 Configuring Basic Printer Scenarios

Using Figure 10 as an example, Table 14 explains the basic steps to configure printers for your Network Stations. Identify the scenario that best meets your needs and follow the steps to configure your printers.

Table 14. Desired Print Scenarios

Desired Print Scenario	Print Job Flow	Configuration Instructions
Network Station to a LAN printer	Network Station A to Printer 4	In the Network Station Manager program, configure an entry in the *Remote Printer Server* field for the LAN printer.
Network Station to a LAN printer with a different datastream	Network Station A to AS/400 server to printer 1	On the server that will transform the print job, create a print device description and queue. The printer device description must contain the IP address or host name of the LAN printer. For more information on configuring a printer device, review the Create Printer Device (CRTDEVPRT) command. In the Network Manager program, configure an entry in the Remote Printer Server field with the IP address or host name of the transform server and its queue name.
Network Station to a locally attached printer	Network Station A to Printer 6	In the Network Station Manager program, configure an entry in the Local Parallel Printer or the Local Serial Printer field, depending on how the printer connects to the Network Station.
Network Station to a locally attached printer with a different datastream	Network Station B to AS/400 Server to Printer 5	On the server that will transform the print job, create a printer device description and queue. The printer device description must contain the IP address or host name of the Network Station to which the printer is attached. For more information on configuring a printer device, review the CRTDEVPRT command. In the Network Manager program, configure an entry in the *Remote Printer Server* field with the IP address or host name of the transform server and its queue name.

Desired Print Scenario	Print Job Flow	Configuration Instructions
Network Station to another Network Station with an attached printer	Network Station B to Network Station A to Printer 6	In the Network Manager program, configure an entry in the *Remote Printer Server* field with the IP address of the Network Station to which the printer is attached. In the *Queue name* field, type PARALLEL1 or SERIAL1, depending on how the printer connects to the Network Station.
Network Station to another Network Station with an attached printer and a different datastream	Network Station A to AS/400 Server to Network Station B Printer 5	On the server that will transform the print job, create a printer device description and queue. The printer device description must contain the IP address or host name of the Network Station to which the printer is attached. For more information on configuring a printer device, review the CRTDEVPRT command. In the Network Manager program, configuration an entry in the *Remote Printer Server* field with the IP address or host name of the transform server and its queue name.
Network Station to a server controller printer	Network Station A to AS/400 Server to Printer 2 or 3	In the Network Manager program, configure an entry in the *Remote Printer Server* field with the host name or IP address that controls the printer. In the *Queue name* field, enter the name of the queue that controls the printer. In this scenario, it does not matter if the datastreams do not match. If you use the CRTDEVPRT command, the server automatically transforms the job if necessary.

2.12.3 Printer Administration Techniques

Administrating a printer environment can be a difficult task. You should create a printer network diagram. Based on your diagram and printing needs, you should develop a printing strategy. Under the right conditions, Network Stations can print to most types of printers.

One technique is to have a server control the printers for your Network Stations. In Figure 10 on page 59, the AS/400 server can control a LAN printer, such as Printer 4. If Network Station A and B always sent their print jobs to the AS/400 server, the AS/400 server can control the flow of print jobs to the printer. This scenario reduces the work load on the Network Stations when the printer's buffer is full because the AS/400 server can negotiate print jobs with the printer. However, handling these print jobs can likely draw on the central processing unit (CPU) of the AS/400 server. This technique can hinder the server's performance depending on the size and frequency of your print jobs. Because you can send the print job from a Network Station, to a server, and then to a printer, this technique also increase network traffic.

A server that controls your Network Station printing is also advantageous in an environment with mixed printer datastreams. Because Network Station applications only generate certain datastreams, you may have to send print jobs to a server, where the print job can be transformed into a datastream that your printer understands. Depending on which application generates the job, you may need to transform your print jobs. This can require more administration in the Network Station Manager program and on the server. Your end users also need to have a better understanding of printing and networking. To eliminate confusion, consider sending all print jobs to the server, regardless of whether the job needs to be transformed. In the end, you will have fewer printer entries in the Network Station Manager program and fewer printer device descriptions on the server.

When you have a server that controls the printers for your Network Stations, you perform less administration, but you sacrifice performance. When a server controls your print jobs, its CPU works harder, possibly slowing performance. Your end users will notice that it takes longer for them to receive their printouts. If you set up your printing strategy to allow your Network Stations to send their jobs directly to the printer (whenever datastream transformation is unnecessary), you can reduce printing time. Because the print job goes directly to the printer, your server does not carry the load of controlling print jobs. Sending your print jobs directly to the printer also reduces the chance of the server misinterpreting your print job. When a server misinterprets a print job, the job may become lost or damaged.

Chapter 3. Using Flash Cards with the Network Station

This chapter outlines the Flash card support for the IBM Network Station, describes how they work with the IBM Network Station, when they should be used and what the limitations are.

Release 3.0 of the IBM Network Station Manager has been enhanced to provide Flash memory card support. This function is available in U.S. English for IBM Network Stations connected to any of the IBM servers supported by Release 3.0.

All the software required to make it operational must be loaded from a server because the IBM Network Station has no disk storage devices. In environments where there is no local server, transferring megabytes of code over a Wide Area Network (WAN) can take 10-20 minutes over a 56kbps line. In order to reduce the time needed to boot in these environments, the Network Station operating system and applications can be stored on a PCMCIA Flash memory card.

Even at larger sites with servers already in place, there may be concerns about server and network loading after a power failure or first thing in the morning when many Network Stations are powered on at once. Servers are very often mission-critical resources. Some customers are reluctant to use them for other purposes which may put unpredictable loads on the server or require excess server capacity that is seldom used, such as after a power failure.

However, if a local server is available at the remote site, it should be used instead of implementing Flash boot technology. Local servers do not have the manageability limitations of Flash boot. These limitations are explained in this chapter.

The Flash memory cards supported are from a select subset of PCMCIA Series D type II cards (listed in the PRPQ P97000, 5799-GEB, Feature Number 4002) and are purchased from several third party vendors. The Flash card product from two of these vendors has been tested and part numbers and card sizings can be found in Section 3.1, “Flash Card Support” on page 64 and in Section 3.1.1, “Flash Card Sizing” on page 65.

In addition to individual IBM Network Stations being able to boot from their own Flash card, the offering also provides the capability for several Network Stations to boot from one Network Station which contains a Flash memory card. This additional function is called *peer boot.*

© Copyright IBM Corp. 1999

3.1 Flash Card Support

The IBM Network Station products only work with linear C series and linear D series PCMCIA type II Flash memory cards. The maximum size of C series technology is limited to 10MB. However, D series cards are currently available in various sizes with up to 32MB of capacity and in the near future will support as much as 40Mbytes of storage capacity.

Flash cards can be purchased from several manufacturers. IBM does not manufacture or resell these cards.

During the residency, we tested Flash cards from Centennial Technologies (http://www.cent-tech.com) and from Simple Technology (http://www.simpletech.com).

Simple Technology offers a full line of D series cards. Centennial Technologies and Simple Technology's part numbers for the various size cards they can supply, that have been tested, are shown in Table 15.

Table 15. PCMCIA Flash Card Part Numbers

PCMCIA Flash Card Size (in Megabytes)	Centennial Technologies Part Number	Simple Technology Part Number
8 Mb	N/A	STI-ST/8AA
12 Mb	PM24138	STI-FL/12AA
16Mb	PM24114	STI-FL/16AA
20 Mb	PM24162	STI-FL/20AA
24 Mb	PM24136	STI-FL/24AA
28 Mb	PM24501	STI-FL/28AA *
32 Mb	PM24265	STI-FL/32AA *
Note: Some Series 100 IBM Network Stations do not function with these Flash cards from Simple Technologies. The Network Station does not boot with the card installed. However, it does boot as soon as the card is removed. IBM is working with Simple to correct the problem.		

Customers who purchased special C/D series Simple Flash memory cards for use with Release 2 of the Network Station Manager program can continue to use these cards.

3.1.1 Flash Card Sizing

Table 16 provides an estimate of the card size required for each IBM Network Station native application. The Series 1000 IBM Network Stations have a different boot kernel. There are also separate executable modules required for supporting the Series 1000. If you intend to peer boot a mixture of Series 1000 and the Series 100 and 300, you need both sets of files and the required card size approximately doubles.

Table 16. Kernel and Application Program Sizes

Function / Application	Size (MB)
Base operating system (mandatory and this figure includes all kernels)	8
3270 Emulator	1
5250 Emulator	2
NC Navigator Browser (does not include JVM)	4
Java Virtual Machine	13
ICA Client	2

The sizes assume that the compressed files (.Z or .z suffix) are used for the kernel and fonts. All of the sizings presume that the login display (ACTLogin) is being used and that all fonts and locale-specific data (keyboards, message catalogs, and so on) are loaded from the server. If locale information is placed on the Flash card, it can require up to 20 MB depending on the application and the locale (this number is even higher for double-byte locales).

Note

ACTLogin or authentication login refers to the process in which a user ID and password is used authenticate a particular user.

You should allow several extra megabytes for future expansion of these files because of the Network Station software enhancements. You should also increase the Flash card size by the size of at least the largest file being put on the card, if there is any plan to update the current card in place.

The numbers are additive. Therefore, the card size for the 5250 emulator is the combination of the size of the (mandatory) Base OS kernel plus the size of the 5250 emulator. Sizes are included for each of the example scenarios in the PRPQ documentation.

The linear Flash memory supported by the Network Station has the characteristic that space is allocated in contiguous blocks at the end of existing used memory. If a file is added or replaced it goes at the end of currently allocated memory and the memory allocated to the previous version of the file is effectively lost.

A utility to reclaim unused space is available but it must be started manually from a command shell locally on the Network Station or remotely by starting a TELNET session to the IBM Network Station.

The PCMCIA Flash cards are formatted using the format utility that is supplied with the Network Station software. Files are then copied to the card using the NFS protocol or by using the local file manager utility on the Network Station. You can also TELNET to the Network Station and invoke the local file manager remotely. It takes approximately two minutes per megabyte to copy data to the Flash card. If the copy process is interrupted, the Flash card may be left in such a state that the Network Station cannot be booted from it and the card will need to be reformatted.

Due to these limitations, we recommend that PCMCIA Flash be treated as read-only memory. While it can be written to by applications (such as a browser), the fact that space is not easily recoverable means that the card will fill up and be unusable for further updates until space is reclaimed manually.

3.1.2 Flash Card Management

The management of the data on a Flash card is time-consuming and is not yet automated. There are no tools provided to synchronize the files on the Flash card with those on the server or even to indicate when the files on the Flash card are down-level from some designated configuration. In fact, the files within the Flash card (local) file system have no timestamps. Therefore, it is not easy to tell which version of each software module is on the card.

A manual Flash card labelling system should to be introduced to identify which level of software and which applications the card contains.

To update the card while it is in the Network Station, it is best to first mount the file system to a server using NFS. Then the new files can be copied (at two minutes per megabyte) to the Flash card. If the link goes down or the card fills up, the card may be left in a partially updated state and render the Network Station unusable until a correctly formatted card is obtained.

For this reason, we recommend that when updates are required, a new Flash card be sent out to the affected sites. The obsolete cards can be returned to be reformatted and Flashed again (file copy) at a central location. This makes

the Flash card similar to CDROM from the administrator's and user's perspective. This arrangement works well as long as the environment is rather static and frequent updates are not required.

3.1.3 Separation of Servers, Authentication Login, and the Flash Card

Beginning in Release 3, the Network Station's NVRAM can be configured so that the kernel is booted from one system, the configuration files are loaded from another system, and user authentication is performed by a third system.

This capability allows a Network Station with Flash memory to be set up so that it boots large, stable files from a Flash memory card and the more volatile configuration files from a centrally-administered server.

User-specific information, such as configuration files, keyboard mapping files, and browser preferences, cannot be easily accommodated on the Flash memory media as there is no way to provide per-user authentication and configuration. Because there is no local user identification and authentication to the Network Station, a server must be in place to provide the correct user specific environment setup such as the home directory, before completing the full start-up of the Network Station.

This restriction does not apply to the case where the Network Station is configured to merely load its operating system locally (using a Flash card) and then transfer control to a server to load specific profiles and applications based on user login. The ACTLogin functionality, combined with separation of servers, enables the full start-up and user configuration of a Network Station when utilizing the Flash memory boot option.

We recommend that separation of servers and ACTLogin be used in all Flash card implementations. The recommended approach is to run Network Station Manager (NSM) at the central or regional site to configure system-wide and user-specific parameters. Then, ACTLogin is started from the Flash card and is used to authenticate the user to the Network Station Manager database on the central site. This results in very low network traffic while keeping the more volatile user files and administration at the central site.

3.1.3.1 ACTLogin Description

The procedure for using Flash with ACTLogin is simple. First, the system and user preferences are configured on the server system using the Network Station Manager program. Then, the kernel and executable modules are loaded on the Flash card. The configuration information is read from the server and augmented by Flash-specific overrides.

By default, ACTLogin attempts to authenticate to the boot server. This obviously will not work correctly when booting from the Flash because there is no default boot server. A specific authentication server must therefore be provided to ACTLogin, as shown in the *flash.nsm* file Figure 13 on page 77.

In some cases, it is desirable to not have the ACTLogin display (for example, login display) show. This is the case if, for example, the user just wants to have an emulator session and ddoes not want to login explicitly to the Network Station to establish personal preferences.

The Network Station can also be configured so that no login and authorization is required. If all Network Stations are going to use the same set of configuration or preference files, then these, along with the executable files, can be placed on the Flash card. Configuration and preference files are small and tend to be somewhat volatile. Therefore, managing them at the server and using separation of servers generally results in less maintenance. In this case, the Flash memory can be set up to hold a generic set of configuration files and application programs. Users then validate themselves directly to the host applications where necessary (an emulation sign on display) when starting an application.

For example, the Network Station Flash memory can be set up to boot the kernel and the 5250 emulator without any user login at the Network Station. However, the user is still required to login to the mainframe after the emulator has been started. Each user of the Network Station would be presented with the same base system, including fonts and keyboard mapping.

Attention

Running the Network Station without using NSM and ACTLogin is not a supported configuration. ACTLogin provides a mode wherein an explicit user login is not required. Refer to Section 1.2.14, “Full-Screen (Kiosk) Solutions Support” on page 20 for information on Kiosk or Full Screen support.

File formats cannot be guaranteed across releases. By using NSM and ACTLogin, you ensure that the system manages most of the data and only executable and stable data reside on the Flash card.

3.1.4 Hardware Considerations

IBM Network Station Series 100 and 300 systems are supplied with built-in PCMCIA adapters. For Series 1000 systems, this adapter is an optional feature on all but the very early Ethernet models. The part number for the

PCMCIA Adapter on the Series 1000 is *07L8336* and can be ordered in the GEMS ordering system in the US and Canada, and the UPOS ordering system in EMEA. Contact your IBM Network Station Sales Representative or Business Partner to order these adapters.

IBM has tested Flash cards from Centennial Technologies (http://www.cent-tech.com) and cards from Simple Technology (http://www.simpletech.com) the latter of which offers a full line of D series cards. Refer to Table 15 on page 64 for a list of current Flash card part numbers available from Centennial Technologies and Simple Technology.

3.2 Booting from a Flash Card with 5250, 3270, and VTxxx Support

In this scenario, we provide a remote site the ability to boot the IBM Network Station and run the 5250, 3270 and VTxxx emulators from the Flash card. This connection is through a slow or heavily utilized WAN. The volatile data is data that is subject to change either on a daily basis or during a software upgrade which is kept on the central system. User authentication using ACTLogin also occurs on the central system.

3.2.1 Scenario Objectives

There are four objectives in this scenario. These objectives are:

- Load the Network Station kernel from the Flash card.
- Load the executable modules for running a 5250, 3270 and VTxxx emulation from the Flash card.
- Use ACTLogin and the server separation function to authenticate the user at the central site.
- Load the user configuration, fonts and other volatile data from the central system, allowing it to be maintained centrally using the IBM Network Station Manager program.

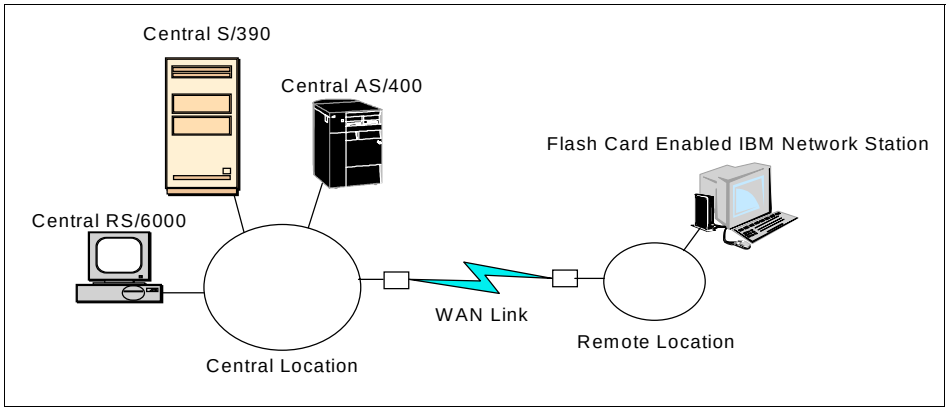


Figure 11. Flash Card Support for Emulators from a Remote Location

3.2.2 Scenario Advantages

The scenario has the following advantages:

- Users at the remote location experience quick boot up times as the required code to start the IBM Network Station is contained on the local Flash card or file system.
- The emulation applications is also located on the Flash card and does not need to be sent across the network.
- The WAN traffic is reduced releasing the bandwidth for other use.
- The volatile user configuration settings continues to be managed on the central server system.
- User authentication is maintained and authenticated on the central server system.
- The use of peer boot is allowed in the future.

3.2.3 Scenario Disadvantages

The following disadvantages apply to this scenario:

- There is no automated central management of the Flash cards.

  The system administrator must ensure that the remote user's Flash card remains up to date when any new releases are applied to the central server system.
- The Flash card is a single point of failure for the remote user.

In the event of a Flash card failure, an identical secondary card should be distributed to the user, along with the first.

- The NVRAM settings cannot be easily changed from local Flash boot to server boot.

  To enable the IBM Network Station to use the Flash card and boot locally, the settings in NVRAM must be modified. It may not be a simple task for the end user to change these settings back in the event of a Flash card failure.

- There is no support in this scenario for the IBM Network Station Series 1000.

  The Series 1000 requires a different kernel and some different module files that do not fit on an 8MB Flash card. You can, of course, use a larger Flash card and support the IBM Network Station Series 100/300 and 1000 series.

3.2.4 Scenario Network Configuration

In this scenario, the IBM Network Station is located at a remote location, distant from the central site which houses the main AS/400, S/390 and RS/6000 systems. The remote location is in the same site, city, or in another geography. There is no local access to the central site systems.

The link from the end user to the central site that is the bottleneck. That is, the communication link is adequate for small bursts of information such as display changes, but has limited file transfer capability due either to the speed, or the utilization on the communication link.

The WAN link is any type, ranging from dial up to frame relay. The actual type of link is not as important in this scenario as long as it can carry TCP/IP traffic.

Figure 12 on page 72 shows the central systems located at the central site and an IBM Network Station located remotely over a slow or possibly congested WAN link.

In this scenario, we used the reserved class A TCP/IP addressing scheme of 10.1.1.X with a subnet mask value of 255.255.255.0, which allows up to 254 devices on this network.

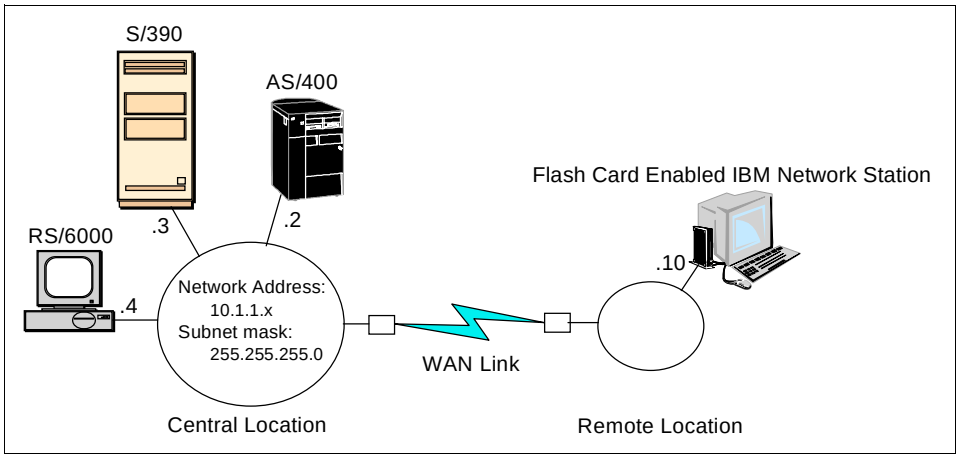


Figure 12. Remote Flash Card Enabled IBM Network Station Topology Diagram

3.3 Creating A Flash Card

To enable an IBM Network Station to boot from the local Flash card, complete the following steps:

1. Verify prerequisite tasks.
2. Create a Flash card boot image.
3. Create a separate configuration file.
4. Test the boot image from the AS/400.
5. Verify functionality.
6. Formatting the Flash Card.
7. Load the Image onto the Flash Card:
   - Using NFS/400.
   - Using the IBM Network Station file manager.
8. Boot the IBM Network Station using the Flash card.
9. Do house keeping.

Note

This scenario makes the assumption that you have already configured one or more menu buttons using Network Station Manager program to enable the 3270, 5250, and VTxxx emulators.

3.3.1 Verifying Prerequisites

You must ensure that your system is running IBM Network Station Manager program Release 3.0 and has the latest PTFs have been installed.

To support Flash cards, you must also have the latest OS/400 and NSM PTF code. The latest PTF for NFS must also be installed if you intend to transfer the data to the Flash card using NFS/400.

3.3.2 Creating a Flash Card Boot Image

To boot from the Flash card, you must first identify the files that are required, copy these files, and test them to ensure that the IBM Network Station will start from this image.

It is necessary to create the image of what will be placed on the Flash card in the Intergrated File System (IFS) of the AS/400 system. This allows you to test booting the Network Station from this image before copying it to the Flash card. After you test the functionality of this image, you can copy it to the Flash card. The process to copy the boot files to the Flash card is rather slow. Data is transferred to the card at a rate of about 2MB per minute.

We recommend that you test the Flash Card before distributing it to the remote office or location. You can perform this test by connecting to a locally attached IBM Network Station.

The following tasks shows how to create an image that contains the files that are required to boot the Network Station, and support the 5250, 3270, and VTxxx emulators. We use the AS/400 system to authenticate the user and provide the font and user configuration files.

The following steps can also be accomplished using Windows 95 and its Explorer function by mapping the AS/400 IFS to a local drive, and using the cut and paste function. The Flash card files can be copied into an *nsflash* image directory on the AS/400 system.

3.3.3 Task Summary

The following steps are required to create a test image that is copied to the Flash card after this testing is successful:

1. Create a test directory structure.
2. Copy the files to the test directory.

3.3.3.1 Creating a Test Directory Structure

By default, the only path in the AS/400 IFS that allows TFTP read access is the default IBM Network Station path, */QIBM/ProdData/NetworkStation*. To avoid changing or altering the *production* directory structure, create an *nsflash* directory in the root of the IFS using the following command, which allows user QTFTP access to this directory:

```
CHGTFTPA ALTSRCDIR('/nsflash')
```

Note: TFTP has no built-in security mechanisms. Use caution to prevent the entire IFS from being exposed to TFTP.

The following steps show how to build and place the Flash card test image in the production directory structure. In this example, we do not create a new directory in the root of the IFS for the test image.

Follow these steps to build a test directory structure:

1. Create a subdirectory in the AS/400 IFS called *nsflash* by entering the following command on any AS/400 command line:

   ```
   CRTDIR DIR('/QIBM/ProdData/NetworkStation/nsflash')
   ```

2. Create a subdirectory under nsflash called *mods* to contain the module files by entering the following command:

   ```
   CRTDIR DIR('/QIBM/ProdData/NetworkStation/nsflash/mods')
   ```

3.3.3.2 Copying the Files to the Test Directory

Use the following steps to copy the files to the test directory structure:

1. From any AS/400 command line type:

   ```
   COPY OBJ('/QIBM/ProdData/NetworkStation/filename')
   TODIR('/QIBM/ProdData/NetworkStation/nsflash')
   ```

   The *filename* is:

   ```
   boot.nsl
   kernel.Z
   ```

Note

In this scenario, we use a Flash card that is only 8MB in size. We only have enough room to place the compressed kernel on this card (denoted by the .Z extension), and not the uncompressed kernel which is about 4MB in size.

Consequently, in this scenario, we do not intend to boot any IBM Network Station Series 1000s from this Flash card.

The files specific to the Series 1000 are denoted by the .63 in the extension. The number 63 relates to the processor found in the Series 1000, the 603e RISC chip.

Appendix A, “Flash Card Scenarios” on page 255 has more information about the files required to support the NC Navigator, Java, and so on, from the Flash card.

2. Copy the module files into the */QIBM/ProdData/NetworkStation/nsflash/mods* directory by entering the following command:

   ```
   COPY OBJ('/QIBM/ProdData/NetworkStation/mods/filename')
   TODIR('/QIBM/ProdData/NetworkStation/nsflash/mods')
   ```

   The *filename* is:

   - actlogin.nws
   - colormap.nws
   - export.nws
   - filed.nws
   - libconf.nws
   - libmlc.nws
   - libprapi.nws
   - libprxapi.nws
   - mcuis.nws
   - miscpr32.nws
   - mwm.nws
   - nfsd.nws
   - ns3270.nws
   - ns5250.nws
   - ns5250xx.nws
   - sbcs_im.nws
   - seriald.nws
   - setup.nws

- term.nws
- nsterm.nws

3.3.4 Creating a Separate Configuration File

To enable the Flash card boot function, make the appropriate changes to redirect the loading of specific files from the AS/400 IFS to the local Flash memory card.

Note

We recommended that you create a new file called *flash.nsm*, rather than edit the supplied system configuration files. The supplied system configuration files can change or be overwritten with each new release of the IBM Network Station Manager program.

The *flash.nsm* file first reads the standard configuration files from the AS/400 server (*standard.nsm*) and then overrides the values as necessary. The flash.nsm file is stored in the */QIBM/ProdData/NetworkStation/configs* directory on the AS/400 server and not on the Flash card. Therefore, any changes that are required must made at a central location and no changes to the Flash card are required.

You can create the *flash.nsm* file can be created using any simple text editor such as Windows Notepad and then copied (using Windows Explorer or using FTP) into the directory */QIBM/ProdData/NetworkStation/configs* in the IFS on the AS/400 system.

The file may also be edited using the stream file editor (EDTF) on the AS/400. The following is a sample *flash.nsm* file for this scenario.

```
# flash.nsm - This file resides in the /QIBM/ProdData/NetworkStation/configs directory
#
# AS/400 File Service Table
#
set file-service-table = {
{"/netstation/prodbase" nil 10.1.1.2 tftp "/QIBM/ProdData/NetworkStation/" unix 3 30
4096 4096}
{"/QIBM/ProdData" nil 10.1.1.2 tftp "/QIBM/ProdData/" unix 3 30 4096 4096 }
}

# Read the configuration files from the server
#
read standard.nsm
#
# Make the necessary mods to the base values
#
set boot-desired-source = tftp
set boot-second-source = none
set boot-third-source = none
set exec-startup-commands = {
{ mcuis }
{ "actlogin -authserv 10.1.1.2" }
}

set file-try-all-matches-on-open = true

# Set up to get executable modules from the Flash card

set modules-directory = /QIBM/ProdData/NetworkStation/nsflash/mods
```

Figure 13. Example Flash.nsm File

3.3.5 Testing the Boot Image from the AS/400 System

To set NVRAM on the IBM Network Station so that it boots using the image located in the IFS that you created in the previous steps, complete the following steps:

1. Reset NVRAM on the IBM Network Station.

   We highly recommend that, before making any major change to the configuration of the IBM Network Station, you reset NVRAM to the factory defaults.

2. Power on the IBM Network Station. The IBM logo is shown, followed by a memory and keyboard check.
3. After the message *NS0500 Search for Host System* is shown, press **ESC** to stop the start-up sequence.

Note

If prompted for an administrator password, enter it now. This is the password an administrator sets using the IBM Network Station Manager program.

4. Start the IBM Network Station Boot Monitor program by pressing the following sequence of keys:
   - For 101/102 keyboards:

     Press and hold **Left Shift + Left Alt + Left Ctrl.** Press **F1**.
   - For 5250/3270 keyboards:

     Press and hold **Left Shift + Left Alt**. Press **F1**.
5. Enter **NV** at the Boot Monitor prompt (>) to access the NVRAM utility.
6. Enter **L** to reset the NVRAM.
7. Enter **S** to save the defaults into NVRAM.
8. Enter **Y** to the question *Are you sure?*
9. Enter **Q** to quit.
10. Enter **SE** (or press F1) from the boot monitor prompt to start the *IBM Network Station Setup Utility.*
11. Press **PF3** (*Set Network Parameters).*
12. The Network parameters should default to *Network* after the reset. To change the *IP Addressed from* field from Network to **NVRAM**, use the right arrow key.
13. Enter the *Network Station IP address*. In this scenario, the IP address of the Network Station is **10.1.1.10**.
14. Enter *The First Boot Host* IP address of **10.1.1.2**. This is the AS/400 system that contains the Flash card image that you want to test.
15. Enter *The First Configuration Host IP address* of **10.1.1.2**. This is the same AS/400 system that contains the Flash card image.

16. Enter the correct IP address information for the fields, *Gateway IP Address* and *Subnet Mask* according to your network. The *Broadcast IP address* should default to the correct setting environment.
17. Press **Enter**.
18. Press **PF4** (*Set Boot Parameters).*
19. Type **kernel.Z** in the *Boot File* field.
20. In the TFTP Boot Directory field, enter the following:

    `/QIBM/ProdData/NetworkStation/nsflash/`

    This forces the Network Station to load the kernel from the Flash card test image. Be sure to include the final slash (/).
21. Leave the *NFS Boot Directory* blank.
22. In the *Boot Host Protocol section*, disable *NFS order* and *Local order* by typing a **D** next to the corresponding field.
23. Enter **1** next to the *TFTP order* field.
24. Press **Enter**.
25. Press **PF5** (*Set Configuration Parameters).*
26. Enter **flash.nsm** in the *Configuration file* field.
27. Enter **/QIBM/ProdData/NetworkStation/configs/** in the *Configuration Directory: First* field.
28. Leave the *Configuration Directory: Second* field blank.
29. Select **TFTP** by using the left or right arrow keys in the *Configuration Host Protocol: First* field.
30. Leave the *Configuration Host Protocol: Second* as default.
31. Press **Enter**.
32. Press **Enter** again to reboot the IBM Network Station.

The IBM Network Station starts and loads the kernel from the */QIBM/ProdData/NetworkStation/nsflash* directory. The *flash.nsm* file points the Network Station to the */QIBM/ProdData/NetworkStation/nsflash/mods* directory to load the emulators and ACTLogin code from.

3.3.6 Verifying Functionality

Verify that the IBM Network Station loads the compressed kernel from the directory */QIBM/ProdData/NetworkStation/nsflash*. You must watch the

Network Station at start up to obtain this information. It can be read from the display after the POST (Power On Self Tests) are complete.

After the Network Station has started up and presented you with the login (*ACTLogin)* display, sign on with the user profile that you have already configured to show the different emulator choices on the menu bar and start each emulator by pressing the appropriate menu bar buttons.

Provided you entered the correct system information when configuring the three emulators using the IBM Network Station Manager program, each one will start and show the appropriate sign-on displays.

Now we must verify that the modules were in fact loaded from the */QIBM/ProdData/NetworkStation/nsflash/mods* directory on the AS/400. This is done by reviewing the console log of the Network Station.

Use the following steps to view the console log and verify that the modules were loaded from the correct directory:

1. Start the emulators by clicking on the button on the task bar of the Network Station desktop.
2. After the emulators have started successfully, press **Alt + Shift + Home** to start the Network Station console.
3. Click on the **Messages** button to view the log.
4. Use the vertical scroll bar to move up and down the log file.
5. Please refer to the following example, which shows in bold text the 5250 emulation executable modules being sourced from the */QIBM/ProdData/NetworkStation/nsflash/mods* directory.

```
Special Command Check, command = ns5250
NSK8202: loading libprapi from
/QIBM/ProdData/NetworkStation/nsflash/mods/libprapi.nws
+ 0:00:08:27
NSK8203: loaded 'IBM Network Station model 8361 V1.3.0 libprapi  07/14/1998, PTF
fix1998290'
NSK8202: loading libprxapi from
/QIBM/ProdData/NetworkStation/nsflash/mods/libprxapi.nws
NSK8203: loaded 'IBM Network Station model 8361 V1.3.0 libprxapi  05/06/1998, PTF DRV190'
NSK8202: loading ns5250 from /QIBM/ProdData/NetworkStation/nsflash/mods/ns5250.nws
+ 0:00:08:32
NSK8203: loaded 'IBM Network Station model 8361 V1.3.0 ns5250  07/14/1998, PTF fix1998290'
+ 0:00:08:33
NSK5901: running command:  ns5250 as1.mycompany.com
NSK8502: host "localhost" connected with blank authorization
+ 0:00:08:35
NSK0603: reading font file: /QIBM/ProdData/NetworkStation/X11/fonts/pcf/i18n/Rom
8.iso1_UCS.pcf.Z
+ 0:00:08:36
NSK8202: loading sbcs_im from /QIBM/ProdData/NetworkStation/nsflash/mods/sbcs_im.nws
NSK8203: loaded 'IBM Network Station model 8361 V1.3.0 sbcs_im  05/06/1998, PTFDRV190'
```

Figure 14. Console Log Example: Loading the 5250 Emulator from the Test Image Directory

After you confirmed that the Network Station was redirected to load the kernel from the */QIBM/ProdData/NetworkStation/nsflash* and the modules from the */QIBM/ProdData/NetworkStation/nsflash/mods* sub directory, proceed with the next step.

If the current directories are not being accessed, review your NVRAM configuration and ensure that the *flash.nsm* file is correct and is being read by the Network Station at start up time by viewing the system log.

3.3.7 Accessing the Local File Manager and NFS

This section describes, in detail, the changes that must be made to the *flash.nsm* file to enable the local file manager and NFS support on the Network Station containing the Flash card. These changes allow you to format and copy the test image(created earlier) to the Flash card.

Use the steps described in the following section to modify the *flash.nsm* file, which enables access to the local file manager and to enable the NFS daemon on the IBM Network Station.

3.3.7.1 Enabling the Local File Manager

To enable the local file manager, perform the following steps:

1. Open the file *flash.nsm* in */QIBM/ProdData/NetworkStation/configs* using a PC editor (or FTP to copy to your PC or AS/400 system and edit locally).
2. Add the following lines to *flash.nsm* after the read *standard.nsm* statement

   ```
   set xserver-initial-x-resources = "ncdconsole.disable.TerminalMenu:
   false"
   set file-manager-password = password
   set file-manager-access-control-enabled = true
   ```

   Replace *password* with the password of your choice.
3. Save the file into */QIBM/ProdData/NetworkStation/configs* and exit.

3.3.7.2 Enabling the NFS Daemon on the IBM Network Station

The following steps enable you to copy the required files to the Flash card using NFS. It is recommended that NFS be used to copy the files to the Flash card. If you intend to use NFS to copy the files to the Flash card, then complete the following steps.

For **NFS support** you must add the following line to the *flash.nsm* file located in */QIBM/ProdData/NetworkStation/configs*.

1. Open the file *flash.nsm* using Wordpad.exe if you have a Windows ’95 client.
2. Add the following line to *flash.nsm* after the read standard.nsm statement

   ```
   set file-enable-nfs-server = true
   ```
3. Save the file into the same directory, */QIBM/ProdData/NetworkStation/configs,* and exit.

3.3.8 Formatting the Flash Card

After you complete the steps in the previous section, and verify that the IBM Network Station started and functions successfully from the test image, you must prepare the Flash card for use and copy the image (created previously) to the Flash card.

You must also complete the previous section to enable the local file manager on the IBM Network Station.

No changes to NVRAM are required at this stage to complete the tasks described in the following section.

3.3.8.1 Using the Local File Manager to Format the Flash Card

We recommend that you format the card prior to use. Use the following steps to verify the Flash card and prepare it for use:

1. Power off the IBM Network Station.
2. Ensure that the write protect switch on the Flash card is in the *enable write* position.
3. Insert the PCMCIA Flash card into the IBM Network Station as recommended by the manufacturer.
4. Power on the IBM Network Station.
5. When the message*NS0500 Search for Host System* appears, press **ESC** to stop the start-up sequence.

   If prompted for an administrator password, enter it now (this is the password an administrator can set using the IBM Network Station Manager program).
6. Press **PF2** (*View the Hardware Configuration)*.
7. Verify that the Network Station has recognized the Flash card is installed.
8. Reboot the Network Station to load the configuration changes made to *flash.nsm* in the previous section.
9. Allow the IBM Network Station start-up to complete. Sign in when the login display is shown.
10. After the desktop has been loaded, start the Console by pressing **Alt + Shift + Home**.
11. Select **Terminals** from the pull down menu options.
12. Select **New Terminal**.
13. Select **File Local —>Connect to the Local File Manager**.
14. Select **OK** (at the bottom left of the display).
15. The Local file manager starts. Enter your password (as defined in step 2 on page 82 using the *set file-manager-password* statement).
16. Type `pwd` to verify that you are in the */local* directory. This is the root of the Flash card.
17. Type `format` to format the Flash card.
18. Answer **yes** to the message:
    Do you want to proceed with formatting [yes | no].

    A message indicates the estimated time it will take to format the Flash card. For example, the format command may state it will take 15 minutes to format an 8Mb card. However, the card should format in 60 to 90 seconds.
19. After the format is complete, please proceed to the next section.

3.3.9 Loading the Image onto the Flash Card

If you completed the steps in Section 3.3.8, “Formatting the Flash Card” on page 82 to build a Flash card from start to finish, the Local File Manager display should be active on your Flash Card enabled IBM Network Station. If the local file manager is not active, follow the previous instructions on how to start it.

There are several tools that you can use to load the image onto the Flash card. You can use NFS/400, NFS from a PC or the IBM Network Station local file manager. There is no FTP daemon on the IBM Network Station. Therefore, FTP cannot be used. NFS/400 has the least number of steps to complete the image transfer the Flash card.

3.3.9.1 Coping Data to the Flash Card Using NFS/400

You can use NFS/400 to copy the files from the IFS on the AS/400 to the Flash card installed in your Network Station. The Network Station has an NFS server daemon and because the AS/400 system is the NFS client, it is *not* necessary to start the NFS servers on the AS/400 system.

Use the following steps to use NFS to copy the required files to the Flash card:

1. Create a directory in the AS/400 IFS to mount the Flash card over by entering `mkdir '/nwslocal'` on any AS/400 command line. Press **Enter**.
2. Mount the Flash card file system over the */nwslocal* directory by entering the following command on any AS/400 command line:

   ```
   MOUNT TYPE(*NFS) MFS('nwsIPaddr:/local/')
   MNTOVRDIR('/nwslocal')
   ```

   The *nwsIPaddr* is the TCP/IP address of the IBM Network Station containing the Flash Card.

Note

If the command to mount the Flash card on the AS/400 fails with the message: *System unable to establish a communication connection to a file server*, please ensure that the line *set file-enable-nfs-server = true* exists in the *flash.nsm* file and that the Network Station has been rebooted. Refer to Section 3.3.8, “Formatting the Flash Card” on page 82 and refer to step 1 on page 82 *Open the file flash.nsm.....*.

3. The *boot.nsl* file, which resides in the path */QIBM/ProdData/NetworkStation/nsflash*, must be edited before copying it to the Flash card.

   a. Open the file *boot.nsl* from the directory /QIBM/ProdData/NetworkStation/nsflash using a PC editor.

   b. Change the following line in *boot.nsl* to read:

      Login.bootConfigType: MOUNT_LOCAL

   c. Close and save the file to the same directory, */QIBM/ProdData/NetworkStation/nsflash*.

4. Enter the following command on any AS/400 command line to copy the *kernel* and *boot.nsl* files to the Flash card:

   ```
   CPY OBJ('/QIBM/ProdData/NetworkStation/nsflash/filename')
   TODIR('/nwslocal') TOCODEPAGE(*CALC)
   ```

   The *filename* is *kernel.Z* and *boot.nsl.*

Note

Remember, the data transfer speed to the Flash card is about 2MB per minute. You can check to see if the copy operation was successful (at any stage) by using the IBM Network Station local file manager and entering the *dir* command to list the current working directory or by entering `df` which will display the local file system and show the numbers of bytes used, remaining and the number of bytes that need to be reclaimed. During a copy operation, you will see the byte count change.

You can also view the file system using the AS/400 command Work Link (WRKLNK) command. However, at the time of writing, the Work Link (WRKLNK) may not show you all the files that reside on the Flash card even though they are there. Work is being done to fix this problem.

5. Create a subdirectory on the Flash card to contain the executable module files by entering the following command on any command line on the AS/400 system:

   ```
   CRTDIR DIR('/nwslocal/mods')
   ```

6. Enter the following command on the AS/400 command line to copy all of the executable modules in to the *mods* directory on the Flash card:

   ```
   CPY OBJ('/QIBM/ProdData/NetworkStation/nsflash/mods/*')
   TODIR('/nwslocal/mods/') TOCODEPAGE(*CALC)
   ```

7. After the copy operation is complete, look for the message on the AS/400 that informs you that all objects were copied and no (or zero) objects failed. You can also use the IBM Network Station local file manager to check that all the files have been copied using the *dir* command.
8. From the Network Station local file manager, type verify on the /local file system. This verifies the file structure and reports back any errors.
9. On the AS/400 command line, enter the following command:

   ```
   UNMOUNT TYPE(*NFS) MNTOVRDIR('/nwslocal')
   ```

10. Power off the IBM Network Station.
11. Remove the Flash card and change the write protect switch to *write protect*.
12. Replace the Flash card according to the manufacturers recommendations.
13. Please proceed to Section 3.3.10, “Booting the IBM Network Station Using the Flash Card” on page 89.

3.3.9.2 Using the IBM Network Station File Manager

You can use the local file manager on the IBM network Station to view and copy files to the local Flash card. The path to the Flash card is */local*. You can also view the IFS directory structure on the AS/400 using the local file manager by changing to the root directory using the command *cd /,* assuming that the host servers have been started on the AS/400.

A full local file manager command list is shown in Table 17 on page 88.

For information about starting the local file manager, refer to Section 3.3.8.1, “Using the Local File Manager to Format the Flash Card” on page 82. Use the following the steps to transfer the Flash test image created in the previous section:

1. Ensure that the host servers are started on the AS/400 by entering the following command on any AS/400 command line:

   ```
   STRHOSTSVR SVR(*ALL)
   ```

2. Type `cd /local` and press **Enter** to ensure that you are in the Flash card file system.
3. Type `mkdir /mods` to create the directory to contain the executable modules.
4. Type `cd /QIBM/ProdData/NetworkStation/nsflash` and press **Enter**.
5. Type **pwd** and press **Enter** to verify your current working directory, which should be `/QIBM/ProdData/NetworkStation/nsflash` as in the previous step.

6. Copy the kernel to the Flash card file system by entering the following command in the local file manager:

   ```
   cp kernel.Z /local/
   ```

   This copy operation should take approximately four minutes to complete.

7. Edit the *boot.nsl* file in */QIBM/ProdData/NetworkStation/nsflash* before copying it to the Flash card.

   a. Open the file *boot.nsl* from the directory */QIBM/ProdData/NetworkStation/nsflash* with a PC editor.

   b. Change the line to read:

      Login.bootConfigType: MOUNT_LOCAL

   c. Close and save the file to the same directory, */QIBM/ProdData/NetworkStation/nsflash*.

8. Copy the *boot.nsl* file to the Flash card file system by entering the following command in the local file manager:

   ```
   cp boot.nsl /local/
   ```

9. Change to the */QIBM/ProdData/NetworkStation/nsflash/mods* directory by entering the command `cd mods` or specify the full path name of */QIBM/ProdData/NetworkStation/nsflash/mods*.

10. Verify your current working directory using the `pwd` command.

11. Type `dir` and press **Enter**. This shows a list of all executable modules that were copied earlier in Section 3.3.2, “Creating a Flash Card Boot Image” on page 73.

    You must copy each file individually, one at a time, from the AS/400 IFS to the */local/mods* directory on the local Flash card file system using the following command:

    ```
    cp filename /local/mods/
    ```

    The *filename* is each of the following names:

    - actlogin.nws
    - colormap.nws
    - export.nws
    - filed.nws
    - libconf.nws
    - libmlc.nws
    - libprapi.nws
    - libprxapi.nws
    - mcuis.nws
    - miscpr32.nws

- mwm.nws
- nfsd.nws
- ns3270.nws
- ns5250.nws
- ns5250xx.nws
- sbcs_im.nws
- seriald.nws
- setup.nws
- term.nws
- nsterm.nws

12. Type **verify** to check the local Flash card file system once the copy operation is complete.
13. Type **df** to display the file system size in bytes.
14. Type **exit** to end the local file manager program.
15. Click on **logout** to end the session.
16. Proceed to Section 3.3.10, “Booting the IBM Network Station Using the Flash Card” on page 89.

Table 17. Network Station Local File Manager Commands

Command	Description
cd *directory*	Changes the current working directory to *directory.*
compare *file1 file2* or **cmp** *file1 file2*	Compare the contents of the two files and displays a message stating whether the files are equivalent.
copy *sourcefile destfile* or **cp** *sourcefile destfile*	Copies the specified file (*sourcefile*) to the specified destination (*destfile*). Copying files may take a long time and affect the kernel's response time while it is taking place. Please see the note at the end of this table.
cwd or **pwd**	Displays the current working directory.
delete *file(s)* or **del** *file(s)* or **remove** *file(s)* or **rm** *file(s)*	Delete the specified *files* from the local file system. On a PCMCIA card, after using the **delete** command, use the **reclaim** command to re-pack previously used file space for subsequent use.
format [/local]	Formats the local file system */local*. **Warning:** Formatting the file system destroys any data that is already on it.

Command	Description
help	Displays a list of Local File Manager commands.
info or **df** [/local]	Lists the total size in bytes of the local file system and the total number of free bytes available.
list or **ls** or **dir** [-R] [*directory*]	Displays a list of the files stored in the local file system. This command can be used with a **-R** option to list subdirectory content recursively.
mkdir *dir_name*	Makes a directory named *dir_name* in the local file system.
quit	Disconnects from the Local File Manager.
reclaim	Reclaims previously used file system space. This command may take several minutes.
verify	Confirms that the local file system structure is valid.
Notes: Before copying files to the local file system from a remote file system, perform the following tasks: 1. On a PCMCIA card, if you deleted files from the local file system recently, use the reclaim command to ensure that all available space is accessible. 2. Make sure that the terminal's file service table includes an entry for the remote location.	

Before copying files from the local file system to a remote file system, consider the following points:

- If you are copying files from the local file system to a remote location, an empty file with the desired name must exist already on the remote file system when using TFTP.
- Write access must be enabled for the file on the remote file system.
- The Network Station's file service table must include an entry for the remote location.

3.3.10 Booting the IBM Network Station Using the Flash Card

After the Flash card is prepared, you can test it and verify that the IBM Network Station can boot from the card.

3.3.10.1 Modify the Flash.nsm File for Local Boot

The *flash.nsm* file in the path */QIBM/ProdData/NetworkStation/configs* must be changed before booting from the Flash card:

1. Open the *file flash.nsm* in */QIBM/ProdData/NetworkStation/configs* using a PC editor.
2. Change the following line from:

   set boot-desired-source = tftp

   to:

   ```
   set boot-desired-source = local
   ```

   and

   set modules-directory = */QIBM/ProdData/NetworkStation/nsflash/mods*

   to:

   ```
   set modules-directory = /local/mods
   ```

3. Ensure the file is saved to the directory */QIBM/ProdData/NetworkStation/config*.

Refer to Figure 15 on page 91 for an updated example of the *flash.nsm* file with all changes and additions made so far.

```
# flash.nsm - This file resides in the /QIBM/ProdData/NetworkStation/configs directory
#
# AS/400 File Service Table
#
set file-service-table = {
{"/netstation/prodbase" nil 10.1.1.30 tftp "/QIBM/ProdData/NetworkStation/" unix 3 30 4096 4096 }
{"/QIBM/ProdData" nil 10.1.1.30 tftp "/QIBM/ProdData/" unix 3 30 4096 4096 }
}

# Read the configuration files from the server
#
read standard.nsm
#
# Make the necessary mods to the base values
#
set boot-desired-source = local
set boot-second-source = none
set boot-third-source = none
set exec-startup-commands = {
{ mcuis }
{ "actlogin -authserv <servIPaddr>" }
}
# Where <servIPaddr> is the AS/400 system IP address, the authentication server.

set file-try-all-matches-on-open = true

# Set up to get executable modules from the Flash card
set modules-directory = /local/mods
#
# The next 4 lines are optional and enable the local file manager which can be accessed using
# TELNET or from the console window on the Network Station.
set xserver-initial-x-resources = "ncdconsole.disable.TerminalMenu: false"
set file-manager-password = nws1red
set file-manager-access-control-enabled = true

# The next line enables the NFS server Daemon for peer boot and is required if the Flash card
# file system is to be mounted to the AS/400 IFS for file transfer.

set file-enable-nfs-server = true
```

Figure 15. Updated Example of the Flash.nsm File

3.3.10.2 Modifying the NVRAM Configuration for Local Boot

To start the IBM Network Station from the local Flash card, the NVRAM setting must be changed.

Use the following steps to start the Network Station from the Flash card:

1. Reset NVRAM on the IBM Network Station

We highly recommend that you reset NVRAM to the factory defaults prior to any major change to the configuration of the IBM Network Station.

a. Power on the IBM Network Station. The IBM logo is shown, followed by a memory and keyboard check.

b. After the message, *NS0500 Search for Host System* appears, press **ESC** to stop the start-up sequence.

   If prompted for an administrator password, enter it now. (This is the password an administrator can set using the IBM Network Station Manager program.)

c. Invoke the IBM Network Station Boot Monitor program by pressing the following key sequence:

   - *For 101/102 keyboards:*

     Press and hold **Left Shift + Left Alt + Left Ctrl**. Press **F1**.

   - *For 5250/3270 keyboards:*

     Press and hold **Left Shift + Left Alt**. Press **F1**.

d. Enter **NV** at the Boot Monitor prompt (>) to access the NVRAM utility.

e. Enter **L** to reset the NVRAM.

f. Enter **S** to save the defaults into NVRAM.

g. Enter **Y** to the question: *Are you sure?*

h. Enter **Q** to quit.

2. Enter **SE** (or press F1) from the boot monitor prompt to start the *IBM Network Station Setup Utility*.
3. Press **PF3** (*Set Network Parameters).*
4. The *IP Addressed from* field should default to **Network** after the factory default reset. Use the right arrow key to change it to **NVRAM**, if required.
5. Enter the *Network Station IP address*; in this scenario the IP address of the Network Station is **10.1.1.10**.
6. Leave *The First Boot Host* IP address setting of **0.0.0.0.**
7. Enter *The First Configuration Host IP address* of **10.1.1.2.** This is the same AS/400 system that contains the Flash card image.
8. Enter the correct IP address information for the fields; *Gateway IP Address, Subnet Mask*. The *Broadcast IP address* should default to the correct setting.
9. Press **Enter**.

10. Press **PF4** (*Set Boot Parameters).*
11. Type **kernel.Z** in the *Boot File* field.
12. Leave the *TFTP Boot Directory* blank.
13. In the *NFS Boot Directory* field, enter **/local/**. This forces the Network Station to load the kernel from the Flash card image.
14. In the *Boot Host Protocol* section, disable *TFTP order* and *NFS order* by typing a **D** next to the corresponding field.
15. Enter **1** next to the *local order* field.
16. Press **Enter**.
17. Press **PF5 (***Set Configuration Parameters).*
18. Enter **flash.nsm** in the *Configuration file* field.
19. Enter in the *Configuration Directory: First* field:

    ```
    /QIBM/ProdData/NetworkStation/configs/
    ```

20. Leave the *Configuration Directory: Second* field blank.
21. Select **TFTP** by using the left or right arrow keys in the *Configuration Host Protocol: First* field.
22. Leave the *Configuration Host Protocol: Second* as default.
23. Press **Enter**.
24. Press **Enter** again to reboot the IBM Network Station.

The IBM Network Station now starts and loads the kernel from the Flash card and the *nsflash.nsm* file (sourced from */QIBM/ProdData/NetworkStation/configs*) file points the Network Station to the */local/mods/* directory on the Flash card from which the emulators and ACTLogin code are loaded.

3.3.11 Verifying Functionality

Verify that the IBM Network Station loads the compressed kernel from the Flash card (/local file system). You must watch the Network Station at start up to obtain this information. It can be read from the display once the POST (Power On Self Tests) are complete. The kernel loads from the Flash card very quickly.

After, the Network Station has started and shown you the login display, sign on with the user profile that you have already configured. This shows the different emulator choices on the task bar. Start each emulator by pressing the appropriate menu bar button.

Provided that you entered the correct system information when configuring the three emulators using the IBM Network Station Manager program, each one starts and the appropriate system sign on display is shown.

Now, you must verify that the modules were loaded from the */local/mods* directory on the Flash card by reviewing the console log of the Network Station.

Use the following steps to view the console log and verify that the modules were loaded from the correct directory:

1. On the IBM Network Station press **Alt + Shift + Home** to start the console.
2. Click on the **Messages** button to view the log.
3. Use the vertical scroll bar to move up and down through the log file.
4. Please refer to the example in Figure 16 which shows in bold text the 5250 emulation executable modules being sourced from the */local/mods* directory on the Flash card.

```
Special Command Check, command = ns5250
NSK8202: loading libprapi from /local/mods/libprapi.nws
+ 0:00:08:27
NSK8203: loaded 'IBM Network Station model 8361 V1.3.0 libprapi  07/14/1998, PTF fix1998290'
NSK8202: loading libprxapi from /local/mods/libprxapi.nws
NSK8203: loaded 'IBM Network Station model 8361 V1.3.0 libprxapi  05/06/1998, PTF DRV190'
NSK8202: loading ns5250 from /local/mods/ns5250.nws
+ 0:00:08:32
NSK8203: loaded 'IBM Network Station model 8361 V1.3.0 ns5250  07/14/1998, PTF fix1998290'
+ 0:00:08:33
NSK5901: running command:  ns5250 as1.mycompany.com
NSK8502: host "localhost" connected with blank authorization
+ 0:00:08:35
NSK0603: reading font file: /QIBM/ProdData/NetworkStation/X11/fonts/pcf/i18n/Rom
8.iso1_UCS.pcf.Z
+ 0:00:08:36
NSK8202: loading sbcs_im from /loacl/mods/sbcs_im.nws
NSK8203: loaded 'IBM Network Station model 8361 V1.3.0 sbcs_im  05/06/1998, PTFDRV190'
```

Figure 16. Console Log Example: Loading the 5250 Emulator from the Flash Card

3.3.12 House Keeping

After you have confirmed that the IBM Network Station started successfully and loaded the necessary modules from the Flash card, we recommend that the *flash.nsm* file be cleaned up to prevent exposure to any security risks.

For example, several lines of text were added to the *flash.nsm* file to allow you to access the local file manager to format the Flash card. You may also have

chosen to use the local file manager to copy files from the AS/400 IFS, instead of using the NFS support.

Use the following steps to change the lines in the file *flash.nsm* to disable access to the local file manager:

1. Open the file using a simple text editor.
2. Delete the following lines from the *flash.nsm* file:

```
set xserver-initial-x-resources =
"ncdconsole.disable.TerminalMenu: false"
set file-manager-password = password
```

3. Modify the line that reads:

```
set file-manager-access-control-enabled = true
```

   to:

```
set file-manager-access-control-enabled = false
```

Note

During the previous steps, the NFS server daemon on the Network Station was also enabled which allowed you to mount the Flash card file system onto a directory in the IFS of your AS/400 system. If you intend to use the peer boot functionality to boot and start other Network Stations from one Flash card-enabled Network Station, then the NFS server daemon must be left enabled. Otherwise, you can turn off the NFS server daemon by completing step 4.

   If support for peer booting is *not* required, follow these steps:

4. Modify the line that reads:

```
set file-enable-nfs-server = true
```

   to:

```
set file-enable-nfs-server = false
```

5. Save the file as *flash.nsm* into the same directory, */QIBM/ProdData/NetworkStation/configs*.

3.3.13 Flash Card Boot Summary

In this section, you created an image in a separate directory in the AS/400 IFS that contained all of the files that were placed onto the Flash card. A new file called, *flash.nsm,* was created and placed into the */QIBM/ProdData/NetworkStation/configs* directory. This file reads the

standard.nsm file and then overrides the values necessary to enable Flash booting. The image was tested by reading the *flash.nsm file* and directing the Network Station, using NVRAM, to load the files and executable modules from the test image.

After the Network Station started and functioned correctly from the test image, the Flash card was formatted and the test image was copied to the Flash card, using either NFS or the local file manager on the Network Station.

Subsequently, file modifications were made to the *flash.nsm* and *boot.nsl* files to load the executable modules from the card, rather than from the test image in the IFS.

The Flash card boot sequence was tested and verified to ensure that the Network Station was using the Flash card correctly.

Finally, lines that are not required for every day use were removed from the *flash.nsm* file.

The Network Station was restarted again to ensure that the changes to the *flash.nsm* file did not adversely affect operation.

3.4 Peer Booting with 5250, 3270, and VTxxx Support

The availability of Flash card support in Release 3 also brings the added functionality of starting other IBM Network Stations from a single Flash card.

Peer boot allows multiple IBM Network Stations located at a remote site (for example, over a slow or highly utilized WAN) to boot from a single Flash card located in another IBM Network Station local to them.

Initial start-up performance for as many as 10 IBM Network Stations booting simultaneously from a single Flash card located in a Network Station on a LAN is quite acceptable.

When Peer boot is utilized, the peer IBM Network Stations load either some or all of the startup files and the executable modules from the serving Network Station, for example, the Network Station with the Flash card.

3.4.1 Scenario Objectives

In this scenario, we want to accomplish the following objectives:

- Configure a Network Station to boot from another Network Station containing a Flash card.
- Load the executable modules required for 5250, 3270 and VTxxx emulators from the Flash card.
- Use ACTLogin and server separation to authenticate the user at the central site.
- Load the user configuration, fonts and other volatile data from the central site, allowing the data to be maintained centrally.

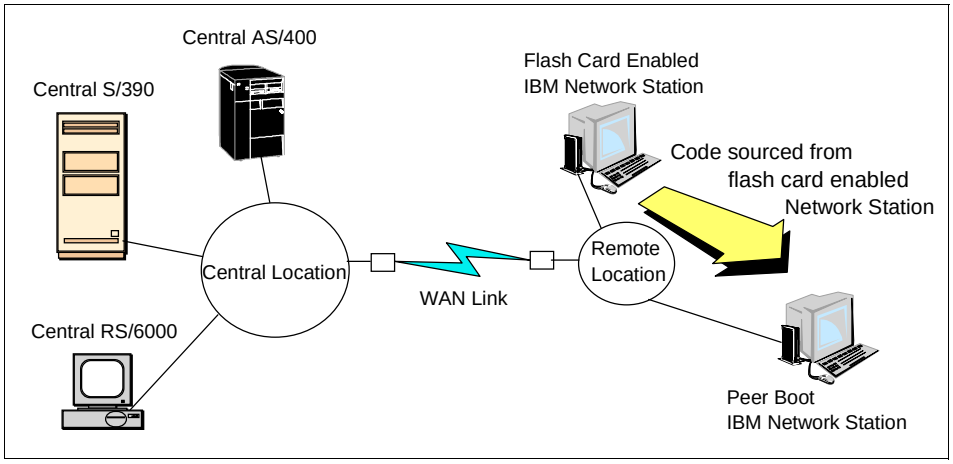


Figure 17. Peer Boot Topology Diagram

3.4.2 Scenario Advantages

This scenario has the following advantages:

- Users at the remote location experience fast boot up times using peer boot.
- The executable modules are contained on the Flash card in the serving Network Station, and are not loaded over the WAN.
- The WAN traffic is reduced.
- User configuration data and preferences remains on the central system, simplifying the management of the data.
- User authentication is maintained and conducted on the central system.

- Only one Flash card is required at each remote location in this case.
- Multiple Network Stations peer boot from the serving Network Station without performance degradation.

3.4.3 Scenario Disadvantages

This scenario has the following disadvantages:

- There is no automated central management of the Flash Cards.

  The system administrator must ensure that the Flash Cards are updated when any new applicable releases and/or Network Station PTFs are applied to the host system.

- The Flash card is a single point of failure for the remote user.

  To improve availability, send a second identical Flash card to the remote site.

- In the event of a Flash card failure, the NVRAM settings cannot be easily changed from local peer boot to server boot.

  To enable the IBM Network Station to peer boot from another Network station containing a Flash card, the settings in NVRAM must be modified. It may not be a simple task for the end user to change these settings back (without assistance) in the event of a Flash card failure.

3.4.4 Network Configuration Scenario

This scenario is similar to the previous Flash Boot section. Once again ,we do not care what type of WAN link that bridges the central business computers with the remote office. This link is of any type, such as dial up serial or Frame Relay, as long as it supports the TCP/IP communication protocol.

However, this link is deemed to be of minimum bandwidth or is perhaps close to being congested and, therefore, unsuitable for larger file transfers. The Flash-card-enabled IBM Network Station acts as a server to the other IBM Network Stations located on the same LAN. The Flash-card-enabled IBM Network Station serves the kernel and other base operating system code to the peer Network Station, as well as the executable modules required to run the different emulators.

The Flash-card-enabled Network Station suffers performance degradation while it serves the kernel and base code to one or more peer Network Stations. After the file transfer is complete, the Flash-card-enabled Network Station continues to function as normal.

The peer Network Station authenticates and load volatile data from the central AS/400 system in the same manner as the Flash-card enabled Network Station.

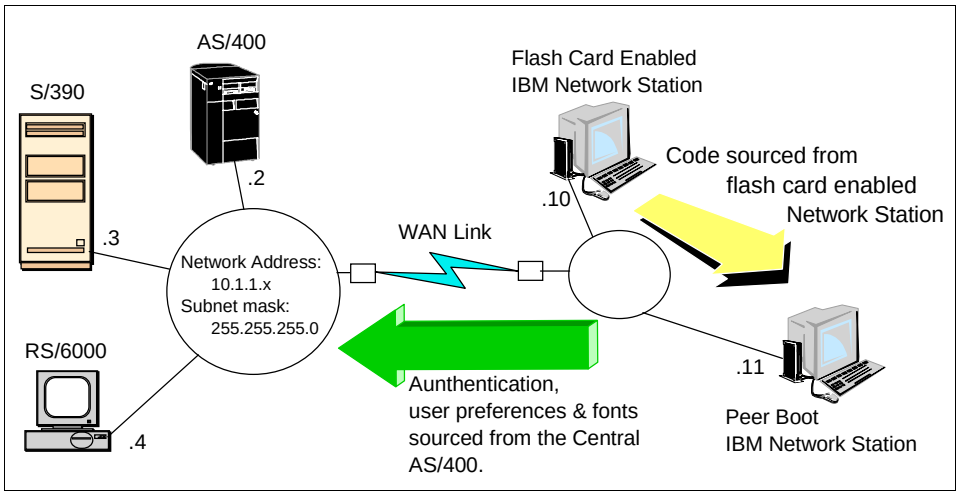


Figure 18. Peer Boot Detailed Network Topology

3.5 Task Summary

To enable an IBM Network Station to load the start-up code and executable modules from a serving Network Station (for example, Peer Boot), the following steps must be completed:

1. Verify Prerequisites.
2. Planning Considerations.
3. Modify the existing Flash boot Network Station.
4. Create a peer boot configuration file.
5. Configure the peer boot Network Station.
6. Test the network Station.

3.5.1 Planning Considerations

Because of the limitations of using a Flash card (such as storage size) to boot the IBM Network Stations, consider the following points:

- What Flash card size is required to support the functions?

  For example, does each user require the same emulation function in the remote office where the Flash card and peer boot functionality is deployed?

If each user using different functions, for example one person requires the Netscape browser, while another requires 5250 and 3270 emulation, then these modules should reside on the Flash card to reduce network traffic and load time.

- Is there a mixture of Series 100/300 and Series 1000 Network stations peer booting from the serving Network Station?

  If there is a mixture of Series 100/300 and Series 1000 Network Stations, should more than one serving Network Station be deployed. Series 1000 requires a different kernel (and other modules) which can exceed the size limitation of the Flash card.

  It is recommended that the Series 1000 Network Stations peer boot from a separate serving Network Station.

- Is redundancy required?

  If all of the people in the remote office are peer booting from one Network Station, then, this system is a single point of failure. A back up Network Station, already configured with another Flash card, should be ready for use if the need arises.

3.5.2 Modifying Existing Flash Boot Network Station Configuration

This scenario assumes you have already configured and tested, or have an existing Network Station that boots or starts from an installed Flash card. If you have not already done so, refer to Section 3.2, “Booting from a Flash Card with 5250, 3270, and VTxxx Support” on page 69.

A change must be made to the *flash.nsm* file which is read from the central AS/400 system. This file must be edited to allow peer boot support.

Use the following steps to enable peer boot support on the serving Network Station which already has the Flash card installed:

1. Edit the file *flash.nsm*, which is located in the directory */QIBM/ProdData/NetworkStation/configs.* Add the following lines of text after the *read standard.nsm* statement:

   ```
   set file-enable-nfs-server = true
   set file-export-directory-list = { { "/peerboot" "/local" } }
   set file-nfs-access-control-default = read-only
   ```

2. Close and save the file.
3. Restart the Network Station that contains the Flash card to invoke the NFS server daemon.

3.5.3 Creating a Peer Boot Configuration File

A new file must be created in */QIBM/ProdData/NetworkStation/configs*, called *peer.nsm*, to distinguish it from the *flash.nsm* file.

This file overrides the normal settings with those required to redirect the Network Station to load executable modules from the Flash card Network Station.

An example of the *peer.nsm* file is shown in Figure 19.

```
# peer.nsm - place into the /local/configs on the Flash card
#
#Set up the file service table to access the server

set file-service-table = {
         { "/netstation/prodbase/configs/" nil 10.1.1.30 tftp "/QIBM/ProdData/NetworkStation/configs/"
unix 3 30 4096 4096 }
          { "/QIBM/ProdData/NetworkStation/configs/" nil 10.1.1.30 tftp
"/QIBM/ProdData/NetworkStation/configs/" unix 3 30 4096 4096 }
         { "/netstation/prodbase/" nil 10.1.1.30 tftp "/QIBM/ProdData/NetworkStation/" unix 3 120 4096
4096 }
          { "/QIBM/ProdData/" nil 10.1.1.30 tftp "/QIBM/ProdData/" unix 3 30 4096 4096 }
}

# Read the base configuration files on the server.
read standard.nsm
#
# Make the necessary mods to the base values

set boot-desired-source = nfs
set boot-second-source = none
set boot-third-source = none
set exec-startup-commands = {
{mcuis }
{ "actlogin -authserv 10.1.1.30" }
}

set file-try-all-matches-on-open = true

#
# Set up to get Java modules, if any from the Flash card

set java-directory = /peerboot/java

#
# Setup to get executable modules from the Flash card

set modules-directory = /peerboot/mods
```

Figure 19. Example Peer.nsm File

The *peer.nsm* file must be placed in to the following path on the serving AS/400: */QIBM/ProdData/NetworkStation/configs*.

3.5.4 Configuring the Peer Boot Network Station

The NVRAM settings on the peer Network Station must be modified to direct it to load the kernel and other configuration data from the Network Station containing the Flash card.

Use the following steps to modify the NVRAM settings on the peer Network Station:

1. Reset NVRAM on the IBM Network Station.

   We highly recommend that you reset NVRAM to the factory defaults before making any major change to the configuration of the IBM Network Station.

2. Power on the IBM Network Station. The IBM logo is shown, followed by a memory and keyboard check.

3. After seeing the message, *NS0500 Search for Host System*, press **ESC** to stop the start-up sequence.

   If prompted for an administrator password, enter it now. This is the password an administrator can set using the IBM Network Station Manager program.

4. Invoke the IBM Network Station Boot Monitor program by pressing the following key sequence:

   - For 101/102 keyboards:

     Press and hold **Left Shift + Left Alt + Left Ctrl**. Press **F1**.

   - For 5250/3270 keyboards:

     Press and hold **Left Shift + Left Alt**. Press **F1**.

   a. Enter **NV** at the Boot Monitor prompt (>) to access the NVRAM utility.

   b. Enter **L** to reset the NVRAM.

   c. Enter **S** to save the defaults into NVRAM.

   d. Enter **Y** to the question: *Are you sure?*

   e. Enter **Q** to quit.

5. Enter **SE** (or press F1) from the boot monitor prompt to start the *IBM Network Station Setup Utility*.

   If you have powered the Network Station off after resetting NVRAM as described these steps, power the Network Station on again. After seeing the message, *NS0500 Search for Host System*, press **ESC** to stop the start-up sequence.

If prompted for an administrator password, enter it now (this is the password an administrator can set using the IBM Network Station Manager program).

6. Press **PF3** (*Set Network Parameters).*
7. The Network parameters should default to NVRAM after the reset. To change the *IP Addressed from* field from Network to **NVRAM**, use the right arrow key.
8. Enter the *Network Station IP address*, in this scenario the IP address of the Network Station is **10.1.1.11**.
9. Enter *The First Boot Host* IP address of **10.1.1.10**. This is the Flash card enabled IBM Network Station.
10. Enter *The First Configuration Host IP address* of **10.1.1.2**. This is the serving AS/400.
11. Enter the correct IP address information for the fields; *Gateway IP Address, Subnet Mask*. The *Broadcast IP address* should default to the correct setting.
12. Press **Enter**.
13. Press **PF4** (*Set Boot Parameters).*
14. Type **kernel.Z** in the *Boot File* field.
15. In the *NFS Boot Directory* field enter **/peerboot/.** This forces the Network Station to load the kernel from the Flash card.
16. Leave the TFTP *Boot Directory* blank.
17. In the *Boot Host Protocol* section, disable *TFTP order* and *Local order* by typing a **D** next to the corresponding field.
18. Enter **1** next to the *NFS order* field.
19. Press **Enter**.
20. Press **PF5** (*Set Configuration Parameters).*
21. Enter **peer.nsm** in the *Configuration file* field.
22. Enter **/QIBM/ProdData/NetworkStation/configs/** in the *Configuration Directory: First* field.
23. Leave the *Configuration Directory: Second* field blank.
24. Select **RFS/400** by using the left or right arrow keys in the *Configuration Host Protocol: First* field.
25. Leave the *Configuration Host Protocol: Second* as Default.

26.Press **Enter**.

27.Press **Enter** again to reboot the IBM Network Station.

The IBM Network Station starts and loads the kernel from the Flash card located in the predefined IBM Network Station.

The file *peer.nsm* points the Network Station to the */local/mods* directory from which the emulators and ACTLogin code are loaded.

Please proceed to the next section to verify that the peer Network Station has sourced the executable modules from the Flash card enabled Network Station.

3.5.5 Verifying Functionality

After you have completed the configuration of the peer Network Station, you must verify that the peer Network Station loaded the code from the Flash card enabled Network Station.

The code, that should be sourced from the Flash card, is the kernel, ACTLogin and executable modules such as the emulators.

Verify that the IBM Network Station loads the compressed kernel from the Flash card (/peerboot file system). You must watch the Network Station at start up to obtain this information. It can be read from the display once the POST (Power On Self Tests) are complete. The kernel loads from the Flash card very quickly.

After the Network Station has started up and presented you with the login display, sign on with the user profile that you have already configured. The different emulators choices are shown on the task bar. Start each emulator by pressing the appropriate menu bar button.

Assuming that you have entered the correct system information when configuring the three emulators using the IBM Network Station Manager program, each one starts and shows the appropriate system sign on display.

Verify that the modules were in fact loaded from the */peerboot/mods* directory on the Flash card, by reviewing the console log of the Network Station.

Use the following steps to view the console log and verify the modules are loaded from the correct directory.

1. On the IBM Network Station, press **Alt + Shift + Home** to start the console.

2. Click on the **Messages** button to view the log.
3. Use the vertical scroll bar to move up and down the log file.
4. Please refer to the example in Figure 20, which shows in bold text the 5250 emulation executable modules being sourced from the */peerboot/mods* directory on the Flash card.

```
Special Command Check, command = ns5250
NSK8202: loading libprapi from /peerboot/mods/libprapi.nws
+ 0:00:08:27
NSK8203: loaded 'IBM Network Station model 8361 V1.3.0 libprapi  07/14/1998, PTF
 fix1998290'
NSK8202: loading libprxapi from /peerboot/mods/libprxapi.nws
NSK8203: loaded 'IBM Network Station model 8361 V1.3.0 libprxapi  05/06/1998, PT
F DRV190'
NSK8202: loading ns5250 from /peerboot/mods/ns5250.nws
+ 0:00:08:32
NSK8203: loaded 'IBM Network Station model 8361 V1.3.0 ns5250  07/14/1998, PTF f
ix1998290'
+ 0:00:08:33
NSK5901: running command:  ns5250 as1.mycompany.com
NSK8502: host "localhost" connected with blank authorization
+ 0:00:08:35
NSK0603: reading font file: /QIBM/ProdData/NetworkStation/X11/fonts/pcf/i18n/Rom
8.iso1_UCS.pcf.Z
+ 0:00:08:36
NSK8202: loading sbcs_im from /loacl/mods/sbcs_im.nws
NSK8203: loaded 'IBM Network Station model 8361 V1.3.0 sbcs_im  05/06/1998, PTF
DRV190'
```

Figure 20. Peer Boot Loading of the 5250 Emulator from the Flash Card

3.5.6 Peer Boot Summary

In this scenario, we had an existing Flash-card-enabled IBM Network Station that we used to serve the kernel and executable modules to another locally attached (for example, on the same LAN) IBM Network Station.

First, we changed the *flash.nsm file* to enable NFS and peer boot support. Subsequently, we built a new file, called *peer.nsm,* which contained the necessary parameters to redirect the peer booting Network Station to the correct target to find the files.

We reset the peer boot Network Stations NVRAM and entered new data in NVRAM to force it to look on the Flash card in the serving Network Station for boot code.

We started the peer boot Network Station and checked the system logs to ensure there were no errors and the Network Station was obtaining the executable modules from the serving Network Station's Flash card.

Chapter 4. Remote Servers and Split Boot Servers

This chapter describes how the split boot feature can be used in different scenarios. These scenarios range from basic to advanced configurations. Please notice that not all of the configurations may apply to your own organization. A mixture of scenarios may better suite your needs.

4.1 Terminology for this Chapter

The following list briefly defines the terms used in this chapter:

Base code server
: This server provides the IBM Network Station with its kernel and support files.

Terminal-based configuration server
: This server provides the IBM Network Station with its *terminal-based configuration settings* (see below).

Authentication and configuration server
: The server is where the IBM Network Station authenticates. It is provided with its *user-based configuration settings*.

Terminal-based configuration settings
: These settings affect the hardware configuration globally and does not pertain to any particular user. Any user default can override these settings.

User-based configuration settings
: These setting provide information about each users configuration. The IBM Network Station Manager program stores this information.

Configuration host IP address
: This is a value that controls from which IP address the IBM Network Station gets its terminal based settings.

Authentication and configuration
: The process that the IBM Network Station performs against the authentication server. Once the user is validated, the IBM Network Station gets the *user-based configuration settings* from the same server.

4.2 Boot Sequence

The following list summarizes each step involved in the Boot sequence (as shown in Figure 21 on page 108).

© Copyright IBM Corp. 1999

1. **Acquire IP address**: It may be already configured into NVRAM or it may be acquired from a DHCP or BOOTP server.
2. **Get the kernel**: The IBM Network Station gets the kernel using several available protocols (tftp, nfs, or local) from the base code server
3. **Get the configuration files**: Usually the *standard.nsm* file from the base code server. However, it can be configured to get this file from another server.
4. **Get the support files**: This loads the needed support files to initialize the Network Station.
5. **Display log-on display**: This gets the *actlogin.nws* and displays the login dialog on the Network Station.
6. **Authentication and configuration process**: This validates the user ID against the default (or otherwise stated) server and gets the configuration files that belong to the validating user from the same server.

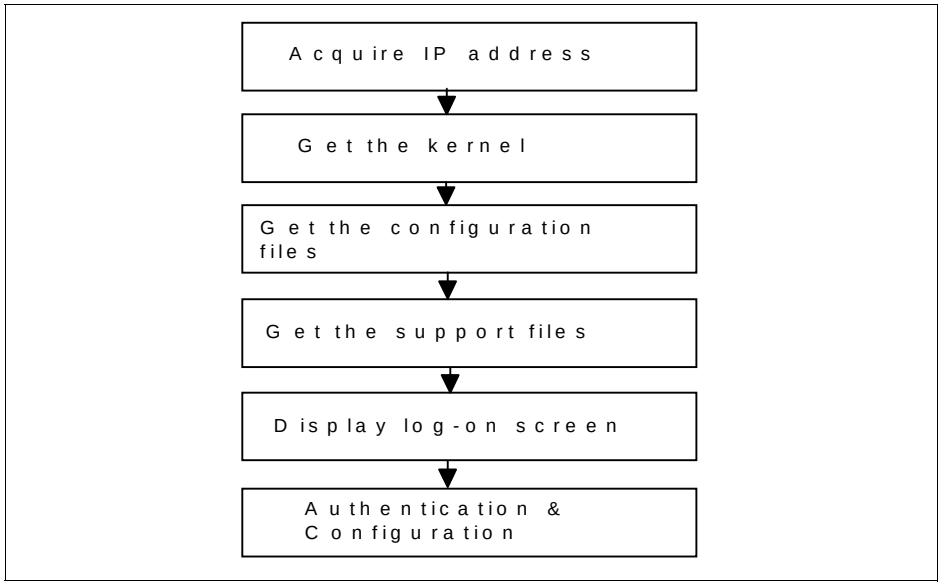


Figure 21. Boot Sequence

4.3 Split Boot Feature

The split boot feature lets you break out the different functions, for example, through separation of servers that the IBM Network Station Manager product would perform on one server as default.

These functions are:

- Base code server
- Terminal-based configuration server
- Authentication and configuration server

The separation of server function in Release 3 allows you to use the split boot feature if you have multiple servers in your organization. The reasons for separating these functions can vary from site to site. The following items are some reasons why you would separate these function:

- **Server consolidation**

  You may want to consolidate all your user data and configuration files on one server.

- **Flash boot**

  Flash cards can only provide basic Boot services. As a result the user authentication and configuration files have to be obtained from other servers.

- **Roaming**

  When you have mobile users, you have the ability for the user to logon with his user-based terminal configuration at any location that supports roaming.

- **Load balancing**

  You may find that a segment or part of your network is not performing. To improve performance you may want to add a server locally, but keep other functions at another site.

4.4 Server Consolidation

In this scenario, we provide an example discussion with a common challenge, server consolidation strategies after initial deployment of IBM Network Stations. You may encounter this situation after deploying the IBM Network Station across your network if your company decides to centralize computing resources, hardware, personnel, and so on.

4.4.1 Scenario Objectives

The following objectives must be achieved to consolidate servers:

1. Start with a distributed configuration and move to a centralized one.
2. Change the authentication and configuration server.

3. Migrate the user-based configuration and data of the users to the new server.

4.4.2 Scenario Overview

In Figure 22, site A, which is the central location (perhaps, headquarters) is connected to the other sites starting from site B, C and so on. In our example, we assume that the initial implementation involved remote boot servers, because the sites were autonomous.

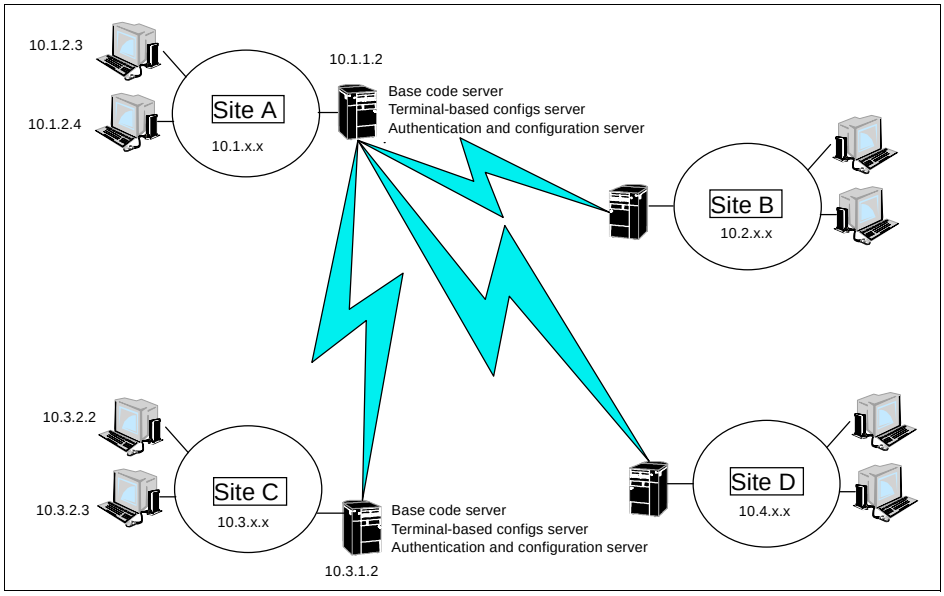


Figure 22. Distributed Server Topology

This is a very common setup because this is how the IBM Network Station Manager program is configured by default. As more Network Stations are deployed, managing many end-user configurations at many sites can become unmanageable. A strategy for improving the management is to split the configuration and authentication from the boot code server. In our example, we concentrate on site C. If needed, the process can be repeated for the other sites as well. As shown in Figure 23 on page 111, the authentication and configuration for users at site C are redirected to the central server at site A.

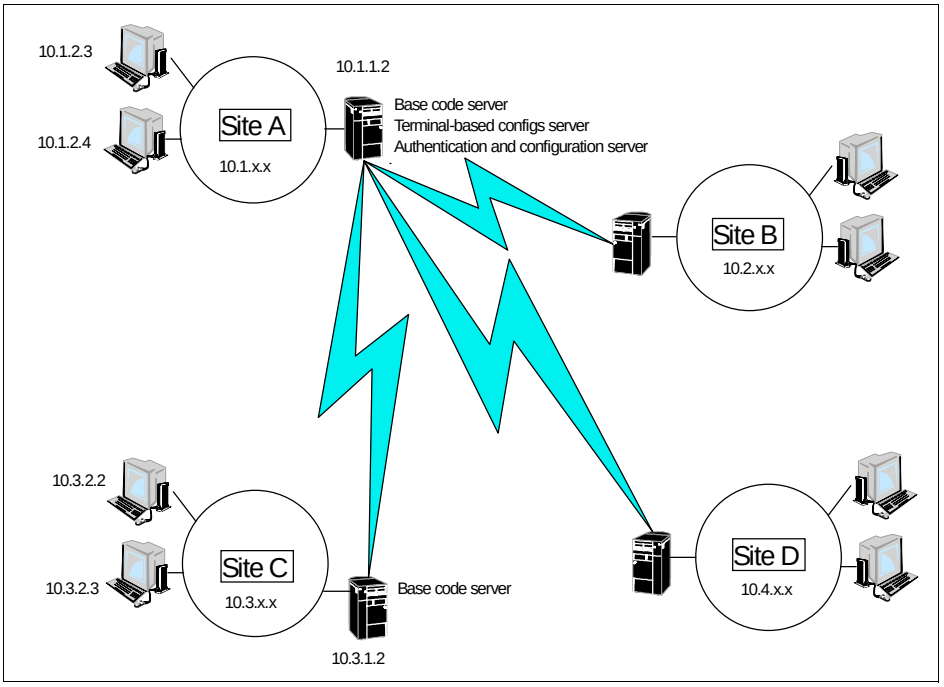


Figure 23. Consolidated Server Topology

4.4.3 Consolidating Servers

To consolidate our authentication and configuration servers, perform the following steps:

1. Change the site C server configuration files to point to the site A server for authentication and configuration, logon to the site C system as an administrator.
2. Copy the authentication and configuration files to a PC using FTP or CA/400 (Client Access/400).
3. Edit the *defaults.dft* file in *QIBM/ProdData/Networkstation/Configs* directory.
4. Add the following statement and ensure that it is the only occurrence of the statement:

```
set exec-startup-commands = {
{ mcuis }
        { "actlogin -authserv 10.1.1.2" }
}
```

In this example, 10.1.1.2 is used in the previous parameter because it is our centralized server's IP address.

After the above steps are completed, users authentication and configuration files come from the centralized server at site A.

Migrate the group or users configuration and data from site C to site A. Site C has the users shown in Figure 24:

- ITSCIDGRPA
- ITSCIDGRPB
- Both belong to group ITSCIDGRP

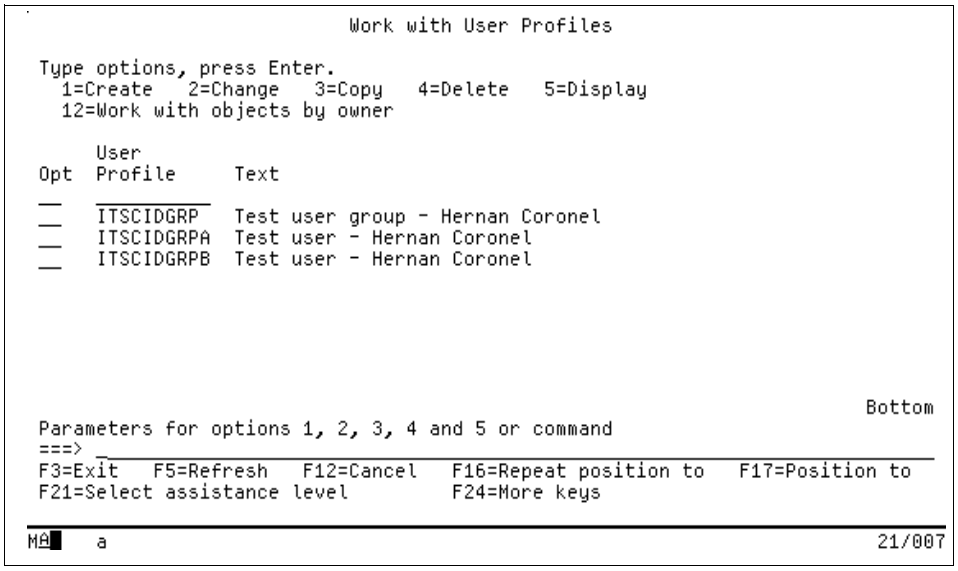

Work with User Profiles
Type options, press Enter.
1=Create 2=Change 3=Copy 4=Delete 5=Display
12=Work with objects by owner
User
Opt Profile Text
ITSCIDGRP Test user group - Hernan Coronel
ITSCIDGRPA Test user - Hernan Coronel
ITSCIDGRPB Test user - Hernan Coronel
Bottom
Parameters for options 1, 2, 3, 4 and 5 or command
===>
F3=Exit F5=Refresh F12=Cancel F16=Repeat position to F17=Position to
F21=Select assistance level F24=More keys
MA a
21/007

Figure 24. Users and User Group

5. To view the attributes of user ITSCIDGRPA, type a **2** under the *Opt* column on the line to the left of *ITSCIDGRPA*.
6. Press **F10** to see more options.
7. Page down once. Notice that the group profile value, *ITSCIDGRP*, indicates that the user belongs to that group.

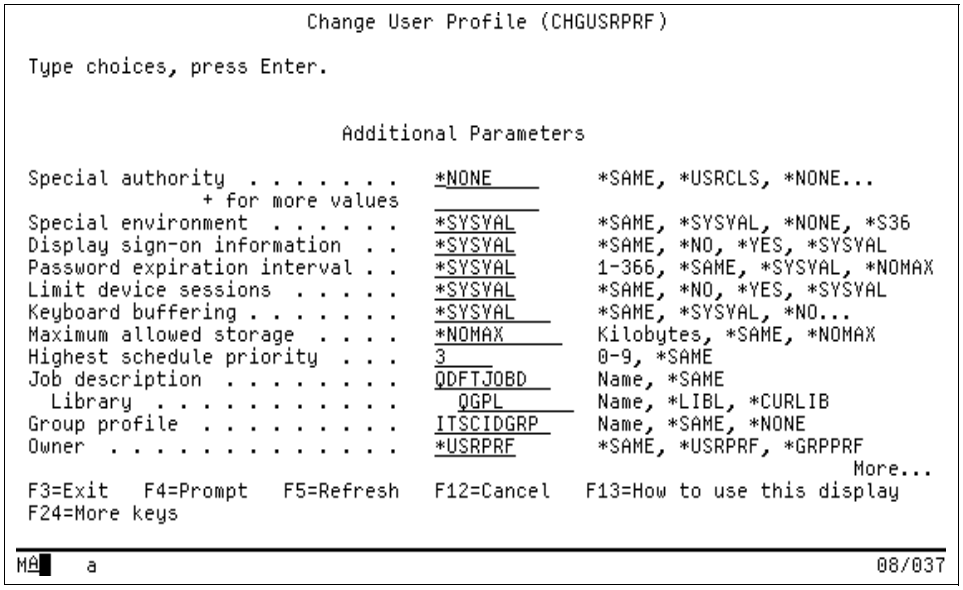

Change User Profile (CHGUSRPRF)
Type choices, press Enter.
Additional Parameters
Special authority . . . . . *NONE *SAME, *USRCLS, *NONE...
+ for more values
Special environment . . . . . *SYSVAL *SAME, *SYSVAL, *NONE, *S36
Display sign-on information . . *SYSVAL *SAME, *NO, *YES, *SYSVAL
Password expiration interval . . *SYSVAL 1-366, *SAME, *SYSVAL, *NOMAX
Limit device sessions . . . . . *SYSVAL *SAME, *NO, *YES, *SYSVAL
Keyboard buffering . . . . . *SYSVAL *SAME, *SYSVAL, *NO...
Maximum allowed storage . . . . *NOMAX Kilobytes, *SAME, *NOMAX
Highest schedule priority . . . 3 0-9, *SAME
Job description . . . . . QDFTJOBD Name, *SAME
Library . . . . . QGPL Name, *LIBL, *CURLIB
Group profile . . . . . ITSCIDGRP Name, *SAME, *NONE
Owner . . . . . *USRPRF *SAME, *USRPRF, *GRPPRF
More...
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys
MA a
08/037

Figure 25. User ITSCIDGRPA

Now create the group profile on site A by completing the following steps:

8. Sign on to the site A AS/400 system using an administrator user ID.
9. At the command line enter the following command and press **F4**:

   CRTUSRPRF

10. Type **ITSCIDGRP** in the user profile field.
11. The password field should be *NONE, because this is a group profile.
12. Type in a text description for this group.

    This should result in a display similar to Figure 26 on page 114.

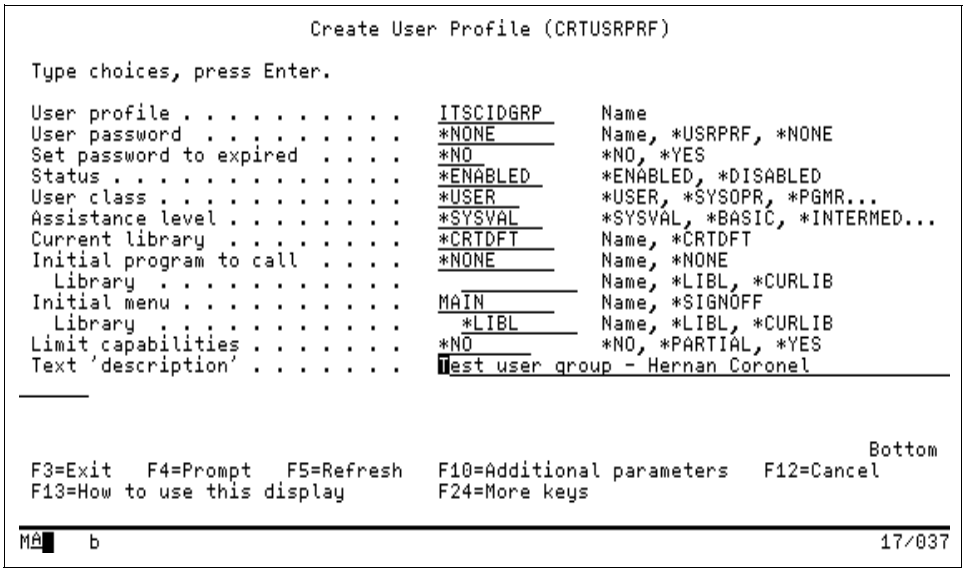

Create User Profile (CRTUSRPRF)
Type choices, press Enter.
User profile . . . . . ITSCIDGRP Name
User password . . . . . *NONE Name, *USRPRF, *NONE
Set password to expired . . . . *NO *NO, *YES
Status . . . . . *ENABLED *ENABLED, *DISABLED
User class . . . . . *USER *USER, *SYSOPR, *PGMR...
Assistance level . . . . . *SYSVAL *SYSVAL, *BASIC, *INTERMED...
Current library . . . . . *CRTDFT Name, *CRTDFT
Initial program to call . . . . *NONE Name, *NONE
Library . . . . . Name, *LIBL, *CURLIB
Initial menu . . . . . MAIN Name, *SIGNOFF
Library . . . . . *LIBL Name, *LIBL, *CURLIB
Limit capabilities . . . . . *NO *NO, *PARTIAL, *YES
Text 'description' . . . . . Test user group - Hernan Coronel
Bottom
F3=Exit F4=Prompt F5=Refresh F10=Additional parameters F12=Cancel
F13=How to use this display F24=More keys
MA b 17/037

Figure 26. Group Creation

Now create the users profile:

13. Type the following command on a command line and press **F4**.

    CRTUSRPRF

14. Type **ITSCIDGRPA** in the user profile field.

15. Type the password in the password field. Ensure that it is the same password on the old system. If it is not, inform the user of the new password.

16. Type the description in the *User class* field.

17. Press **F10** for more options.

18. Page down to scroll down.

19. Type in a user description in the *text description* field.

20. Go back to step 13 and create user profile ITSCIDGRPB.

    The following figures show the creation of user profile ITSC10GRPA.

```
                    Create User Profile (CRTUSRPRF)

 Type choices, press Enter.

 User profile . . . . . > ITSCIDGRPA    Name
 User password  . . . . . > password_    Name, *USRPRF, *NONE
 Set password to expired  . . . .  *NO  *NO, *YES
 Status . . . . . .  *ENABLED    *ENABLED, *DISABLED
 User class . . . . . .  *USER   *USER, *SYSOPR, *PGMR...
 Assistance level . . . . . .  *SYSVAL   *SYSVAL, *BASIC, *INTERMED...
 Current library  . . . . . .  *CRTDFT   Name, *CRTDFT
 Initial program to call  . . . .  *NONE   Name, *NONE
   Library  . . . . . .  _________  Name, *LIBL, *CURLIB
 Initial menu . . . . . .  MAIN   Name, *SIGNOFF
   Library  . . . . . .  *LIBL   Name, *LIBL, *CURLIB
 Limit capabilities . . . . . .  *NO   *NO, *PARTIAL, *YES
 Text 'description' . . . . . > 'Test User'
_____

                                                                    More...
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys

 MA_   b                                                        06/045
```

Figure 27. User's Attributes (Part 1 of 2)

```
                    Change User Profile (CHGUSRPRF)

 Type choices, press Enter.

                          Additional Parameters

 Special authority  . . . . . .  *NONE     *SAME, *USRCLS, *NONE...
             + for more values    _____
 Special environment  . . . . . .  *SYSVAL   *SAME, *SYSVAL, *NONE, *S36
 Display sign-on information  . .  *SYSVAL   *SAME, *NO, *YES, *SYSVAL
 Password expiration interval . .  *SYSVAL   1-366, *SAME, *SYSVAL, *NOMAX
 Limit device sessions  . . . . .  *SYSVAL   *SAME, *NO, *YES, *SYSVAL
 Keyboard buffering . . . . . .  *SYSVAL   *SAME, *SYSVAL, *NO...
 Maximum allowed storage  . . . .  *NOMAX    Kilobytes, *SAME, *NOMAX
 Highest schedule priority  . . .  3        0-9, *SAME
 Job description  . . . . . .  QDFTJOBD   Name, *SAME
   Library  . . . . . .  QGPL     Name, *LIBL, *CURLIB
 Group profile  . . . . . .  ITSCIDGRP_   Name, *SAME, *NONE
 Owner  . . . . . .  *USRPRF   *SAME, *USRPRF, *GRPPRF
                                                                    More...
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys

 MA_   b                                                        19/046
```

Figure 28. User's Attribute (Part 2 of 2)

Now we need to migrate configurations and data.

We are going to use a PC with Windows 95 and CA/400 connected to an AS/400 in this example. To continue, we need to have the AS/400 connections folder from CA/400 already configured.

21. Select **Tools** from the Explorer menu.
22. Select the **Map Network Drive** menu option.
23. Map any available drive letter to the site C host name preceded by two backslashes. In our example, it is drive F: to \\MYSERVER.
24. Map any available drive letter to the site A host name preceded by two backslashes. In our case, it is drive G: to \\MYSERVER. In both cases, you can leave the *Reconnect at logon* option unchecked
25. Start with the group's configuration files on the site C server. Select **F:—> QIBM —> UserData —> NetworkSation —> Groups —> ITSCIDGRP** folder on the left pane. Press the right mouse button over the folder and select **Copy**.
26. Select **G:—> QIBM —> UserData —> NetworkSation —> Groups** folder on the left pane. On the right pane right-click over a white area and select **Paste**, as shown in Figure 29 on page 117.

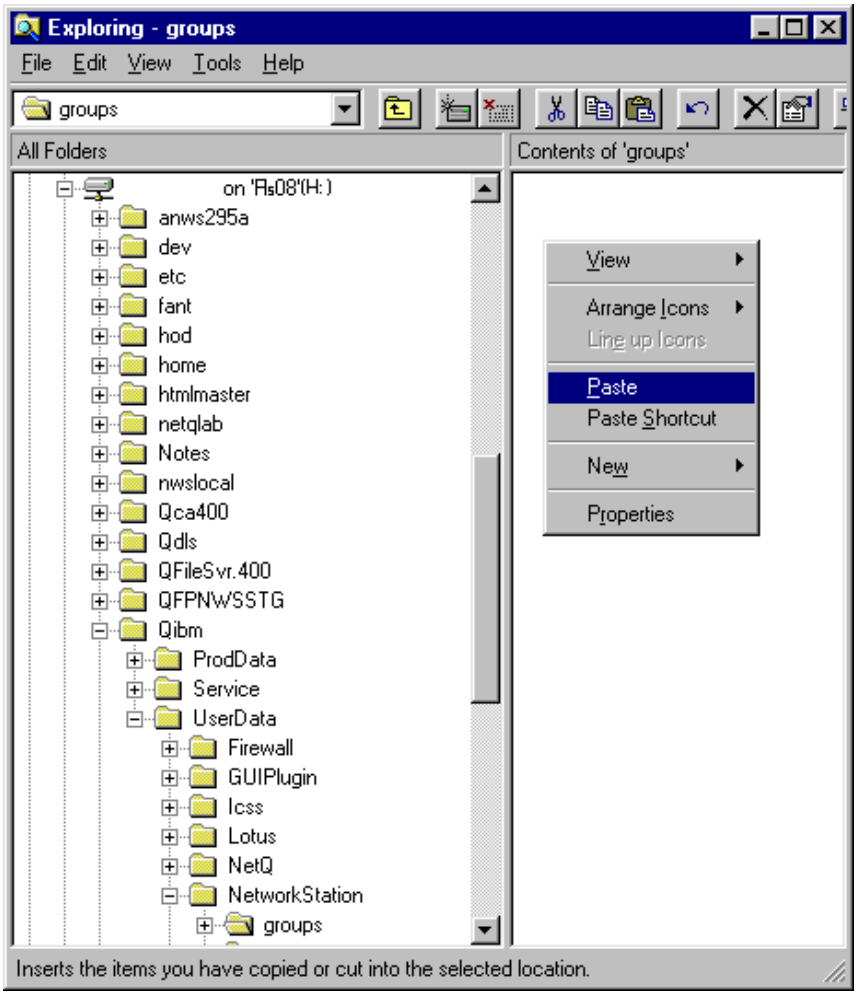


Figure 29. Paste Group's Configuration Files

The group configuration files should be copied, as shown in Figure 30 on page 118.

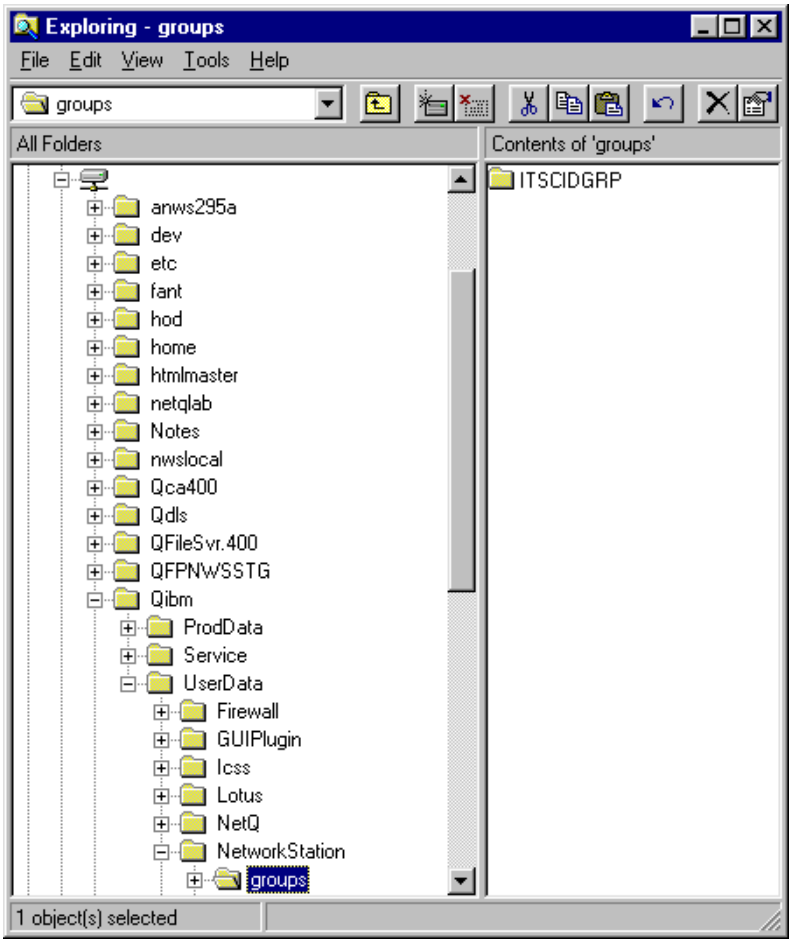


Figure 30. Resulting Group's Configuration Files

In the next steps, the user configuration files are copied.

27. Select the **F:—> QIBM —> UserData —> NetworkStation —> Users —> TSCIDGRPA** folder on the left pane. Press the right mouse button over the folder and select **Copy**.

28. Select the **G:—> QIBM —> UserData —> NetworkStation —> Users** folder on the left pane. On the right pane right-click over a white area and select **Paste**.

29. Repeat the above two steps using ITSCIDGRPB. Select the **F:—> QIBM—> UserData —> NetworkStation —> Users —> TSCIDGRPB**

folder on the left pane. Press the right mouse button over the folder and select **Copy**.

30. Select the **G:—> QIBM —> UserData —> NetworkStation —> Users** folder on the left pane. On the right pane, right-click over a white area and select **Paste**.
31. Finally you have to copy both user data folders, which are in **F:—> QIBM —> UserData —> NetworkStation —> Home —> ITSCIDGRPA** and **F:—> QIBM—> UserData —> NetworkStation —> Home —> TSCIDGRPB**. These subdirectories may not exist. If they do, proceed through steps 32 through 35.
32. Starting with ITSCIDGRPA. Select the **F:—> QIBM—> UserData —> NetworkStation—> Home —>I TSCIDGRPA** folder on the left pane. Press the right mouse button over the folder and select **Copy**.
33. Select the **G:—> QIBM—> UserData —> NetworkStation —> Home** folder on the left pane. On the right pane, right-click over a white area and select **Paste**.
34. Now user ITSCIDGRPB. Select the **F:—> QIBM —> UserData —> NetworkStation —> Home —> ITSCIDGRPB** folder on the left pane. Press the right mouse button over the folder and select **Copy**.
35. Select the **G:—> QIBM —> UserData —> NetworkStation —> Home** folder on the left pane. On the right pane right-click over a white area and select **Paste**.

    As a result of doing the above tasks, the distributed users in site C can boot locally from their server, but are managed (for example, authenticated) from the central server at site A.

Note

Be careful not to overwrite other user's data that may exist.

For example, let us assume that before doing the migration, you have a user called *cashier1* defined on AS/400 systems at site A and B. When you try to migrate *cashier1's* configuration from site B to site A, you will overwrite Site A *cashier1's* configuration because they both sit at \QIBM\UserData\NetworkStation\users\cashier1 or \QIBM\UserData\NetworkStation\groups\cashier1. Be sure to plan ahead and choose your user profile names carefully.

4.5 Roaming Feature

The roaming feature allows mobile users (for example, users that are not at their home systems) to use the facilities of a remote system to access their local user-based terminal setup.

At the Network Station login dialog screen or display there is a *Roam* button that allows you to locate your home configuration files. The user that is visiting New York can still authenticate and get his desktop settings from his home server in Chicago and boot from the local system, therefore, saving management overhead, bandwidth utilization, and time.

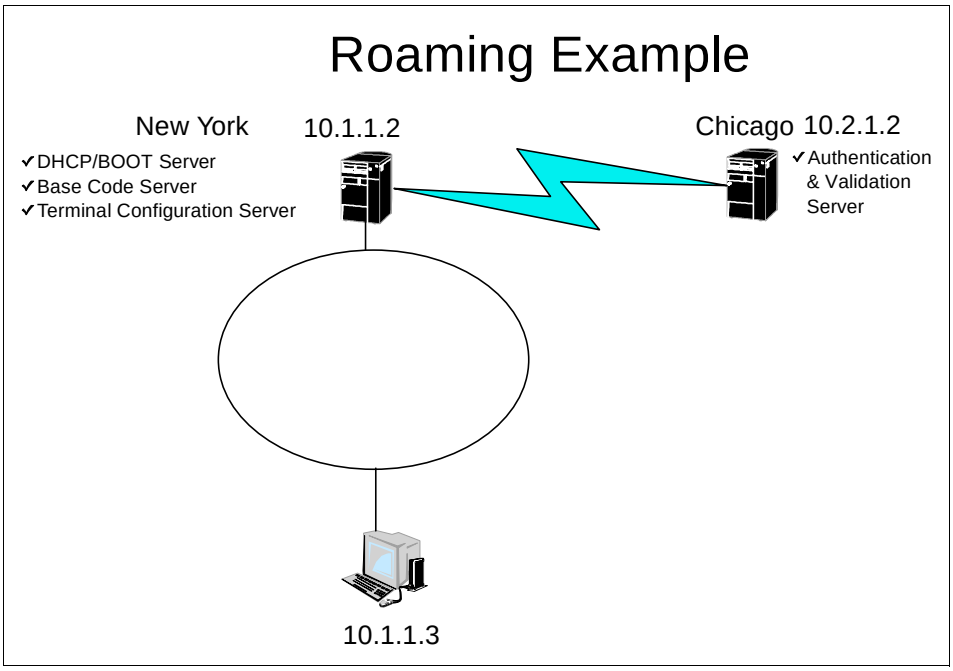


Figure 31. Roaming Example

In Figure 31, a user from Chicago is visiting the New York site. There are servers in both Chicago and New York.

The server in New York provides the following to the Network Station:

- The IBM NetworkStation's IP address
- The operating system and applications
- The terminal-based configuration information
- A login dialog or display

After the Network Station has booted up, the visiting user selects the *Roam* button on the login dialog. The user then enters the name or address of the Chicago authentication server (such as *nsm1chicago.mycompany.com* or *10.2.1.2*).

As a result, the Chicago authentication server validate or authenticates the user ID and password entered, and downloads any user based configuration information.

Although the IBM Network Station Manager program on the server in Chicago manages the user-based configuration information, the IBM Network Station Manager program on the New York server manages the terminal-based user configuration.

Roam Feature and Configuration Host IP Address from NVRAM

Although it seems that Roam feature and the configuration host IP address from NVRA are essentially the same, this is not actually the case. The configuration host IP address is static and the Roam feature is dynamic.

The Roam feature is for mobile users that want to login to a remote system and access their desktop configuration (user-based settings) wherever they are. On the other hand, the configuration host IP address option in the hardware setup utility is used to obtain terminal-based configuration settings. These two features are not the same and cannot be used interchangeably.

4.5.1 Managing User Configurations at Each Remote Site

There are basically three strategies for building and maintaining user configurations at remote sites.

4.5.1.1 Fully Centralized Configuration

In this basic model (see Figure 32 on page 122), the Network Stations obtain everything from the centralized server.

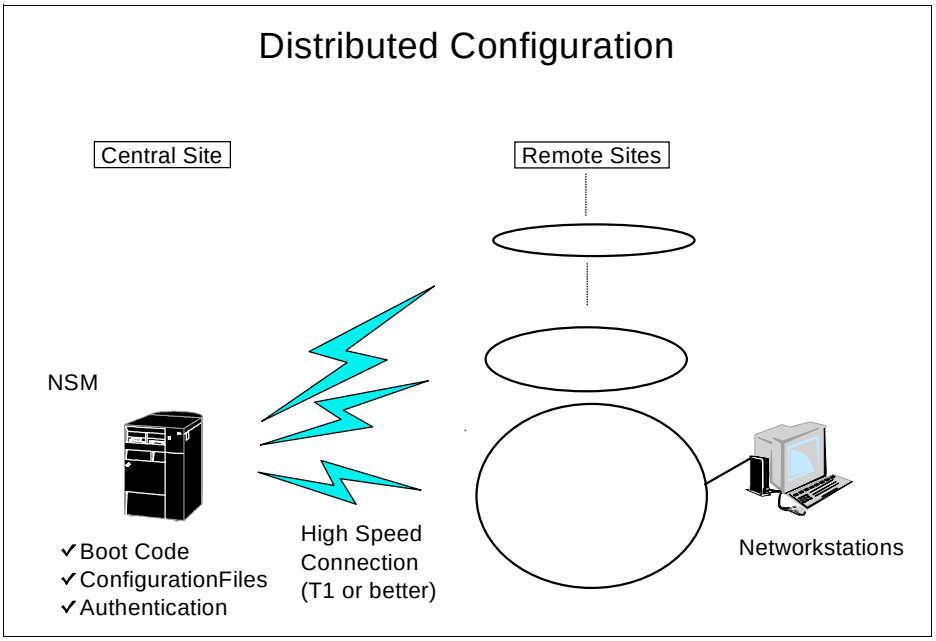


Figure 32. Fully Centralized Configuration

The advantages for this strategy are:

- Centralized server management
- Centralized configuration for all clients
- Fewer servers to deploy and manage
- Reduced hardware costs (due to fewer servers)

However, there are several significant disadvantages:

- A very high bandwidth connection between the sites (T1 or better) is needed.
- If the link goes down, the central site is unavailable.
- The time required to download the operating system to the Network Station could be 10 to 20 minutes, even on a 56k line.

Although the above configuration may apply to some customers, it is not common for a Network Station implementation. This is a common configuration for NPTs connected to a mainframe. The main disadvantage of the this scenario, is that if the link goes down, your remote sites are rendered useless.

4.5.1.2 Remote Boot with Centralized Configurations

This example, is perhaps the most common configuration (see Figure 33).

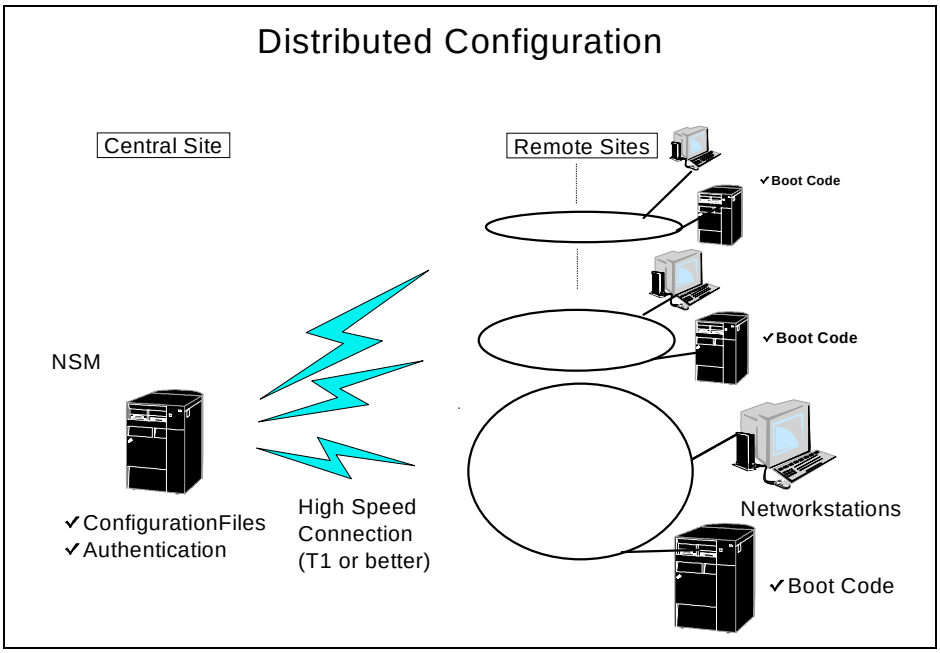


Figure 33. Remote Reboot with Centralized Configurations

By deploying a boot server at each remote site, we get better usage of the remote and local bandwidth available. We use the remote bandwidth to get the configuration files from the central server and the local LAN to get the base code. In this scenario, the user configuration settings are still centralized on the main server.

The advantages of this strategy are:

- Centralized configuration management
- Lower bandwidth connection
- Faster boot

The disadvantages for this strategy are:

- More hardware is needed
- Somewhat decentralized (more servers to manage, potentially one per site)

4.5.1.3 Remote Boot Servers Provide All Functions

Remote boot servers are used to provide all functions (such as boot, authentication, and so on) to the Network Station.

The advantages for this strategy are:

- Independent from central authentication servers (for example, if the link goes down)
- Smaller bandwidth required
- Faster bootup
- Remote servers can be used to deploy other applications

The disadvantages for this strategy are:

- More hardware required
- More servers to deploy and manage

4.5.2 Centralized versus Distributed

If you have a distributed site model, it can appear as shown in Figure 34.

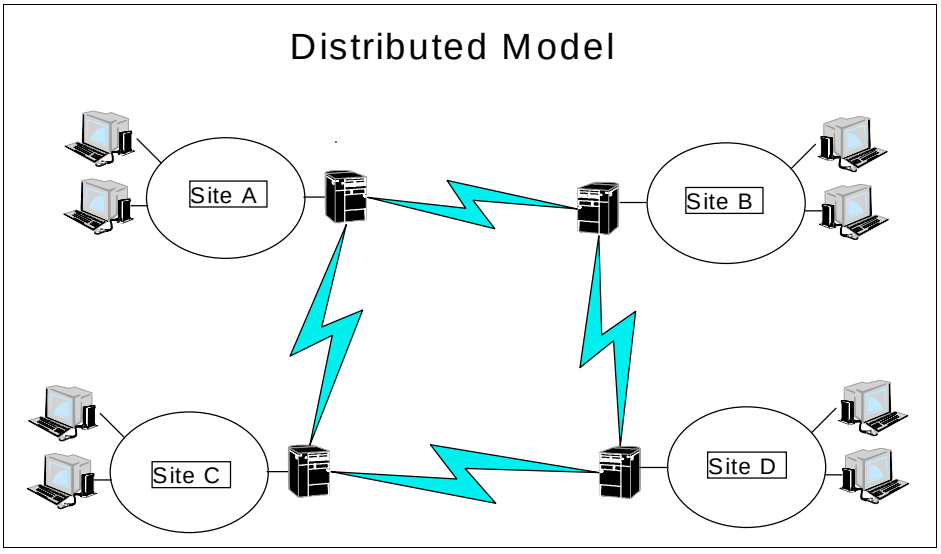


Figure 34. Distributed Model

In this example, you can see that each of the sites is connected by some kind of WAN link that enables them to share information. Each of the sites is independent having the applications, configuration and data locally. While this usually brings a high level of availability, it also brings a high level of management overhead, thus increasing the *total cost of ownership*.

If you are using a centralized model, it can appear as shown in the Figure 35.

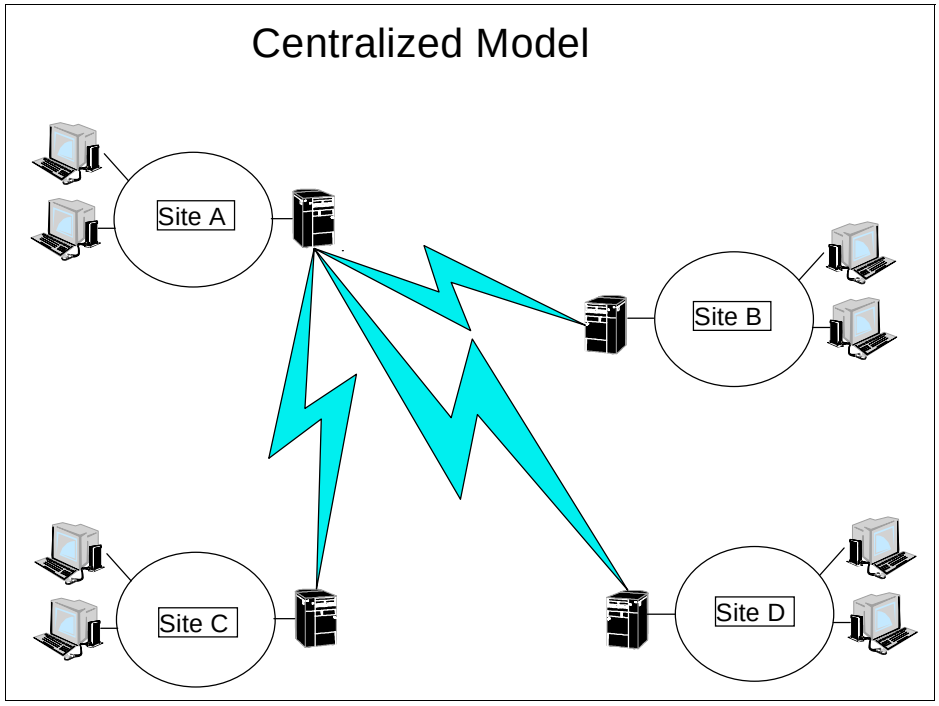


Figure 35. Centralized Model

In Figure 35, every site is connected to site A and every remote site has a local server. For example, a bank or insurance company may keep their branch office data local (for example, in the remote servers), but may transfer updated statistics or prices from the central location. Another variation can result because of the size of the different remote branches. While large remote branches may have a server, like an AS/400 system, for booting Network Stations. For applications serving, smaller branches may have a PC Server or no server at all. They may boot from a Flash card, and then transfer the rest of the code from the central site.

The examples in this chapter depict relatively few remote sites. However, you may have hundreds or thousands of remote sites in your enterprise. In this case, it is even more critical to do the appropriate planning before implementation.

Your current situation and future business needs dictate which of the models discussed in this chapter are best suited your environment. Each has its

advantages and disadvantages. In general, the distributed model is the opposite.

The advantages of the centralized model are:

- Less management overhead
- Reduced hardware costs
- Reduced hardware deployment costs
- Reduced application deployment costs

The disadvantages of the centralized model are:

- Some data or applications may not be accessible if the link goes down .
- Increased communication costs (for example, higher bandwidth).
- Increased cost in communication hardware.

Chapter 5. Twinax Attachment of Network Stations

The non-programmable terminal (NPT) has, traditionally, been one of the user interfaces to an AS/400 system. The NPT's limited capabilities however, has prevented it from connecting to an intranet or Internet. For such connectivity, a personal computer (PC) would be considered but with an associated cost for PC hardware, software, on-going maintenance, support costs and possibly additional wiring. A low cost solution is needed in an environment where NPT users may require internet access. The answers, for this scenario, came initially with the ability to run the TCP/IP protocol encapsulated within Twinaxial Data Link Control frames (available with V4R2 OS/400) and secondly with the availability of the IBM Network Station Twinax models.

5.1 Use of Twinax Attached Network Stations

In AS/400 twinax environments, where there is a need to upgrade the existing NPTs for increased function, the IBM Network Station Twinax model is a solution worth considering.

For customers choosing the IBM Network Station Twinax model, it is easier to:

- Take advantage of the cost-effectiveness of NPTs with simultaneous access to applications using 5250, 3270, or VTxxx emulation.
- Use company intranets or the Internet using the NC Navigator.
- Access Windows applications using a multi-user Windows NT based server.

These same customers can consider the following points:

- No twinax rewiring is needed.
- No additional hardware changes are required on the AS/400 system.
- Having a mixture of NPTs, PCs and Network Stations on the same AS/400 workstation controller.

If the IBM Network Station Twinax model is considered, the customer must understand that:

- Some AS/400 TCP/IP knowledge is required for the setup of these twinax Network Stations.
- The twinax Network Station cannot act as a primary console. However, it can operate as a secondary console.
- The twinax Network Station cannot be attached to an IBM 5494, 5394, or 5294 remote workstation controller.

© Copyright IBM Corp. 1999

For further information regarding the IBM Network Station Twinax model, visit the Web site: http://www.pc.ibm.com/networkstation. Clicking on the *Support and Services* tab will present a link to the IBM Network Station Release 3.0, which contains detailed information on the Model 341.

5.2 AS/400 Software Requirements

The AS/400 software must meet the following requirements:

- OS/400 level must be V4R2 or higher
- Cumulative PTF package C8140420 or later

5.3 AS/400 Hardware Requirements

Both the express and non-express types of work station controllers can be used in an environment to support IBM Network Station Twinax models.

The non-express adapters, which were available on systems before V4R1, are types 6050 and 6140.

The express adapters include:

- 2720 (also known as a 266C)
- 2722
- 6180

In general, all work station controllers (WSC), shipped since V4R1, have at least one of the above express adapters installed.

There are a number of distance limitations on any twinax workstation controller when used in express mode. Refer to the following Web site for further information: www.networking.ibm.com/525xpres/525xwire.html

5.4 Basic IP over Twinax Scenario

This particular scenario shows how to get started with IP over twinax. It demonstrates how to configure a simple environment where one AS/400 system has IBM Network Stations attached by way of twinax.

This scenario attaches the twinax IBM Network Stations to a local workstation controller on the AS/400 system. The local workstation controller is CTL01, which also supports the system console.

5.4.1 Scenario Overview

This scenario shows an example of a twinaxial Network Station subnet attached to an AS/400 system. This same AS/400 server has connectivity to a LAN.

There is a minimum configuration needed on the Network Stations and some TCP/IP configuration required on the AS/400 system. A private set of IP addresses is used for the twinax subnet.

5.4.2 Scenario Objectives

The objectives of this scenario are to:

- Configure the twinax attached IBM Network Stations.
- Configure the AS/400 server to allow connectivity of these twinax IBM Network Stations.

5.4.3 Scenario Advantages

The advantages of this scenario are:

- It is easy to implement.
- The twinax-attached Network Stations can access the Web server on the AS/400 system (if configured). An express adapter, although not mandatory, is recommended in this type of configuration.

5.4.4 Scenario Disadvantages

The disadvantages of this scenario are:

- No consideration has been given to the future growth of the TCP/IP network on the AS/400 server.
- Some TCP/IP knowledge is required to configure the necessary elements on the AS/400 system.
- The twinax attached Network Stations cannot communicate with any hosts beyond the AS/400 server.

5.4.5 Scenario Network Configuration

Figure 36 on page 130 shows the network topology of the simple TCP/IP network. The AS/400 system has connectivity only to an internal LAN. A different network is used for the twinax subnet. This network is 10.10.10.0.

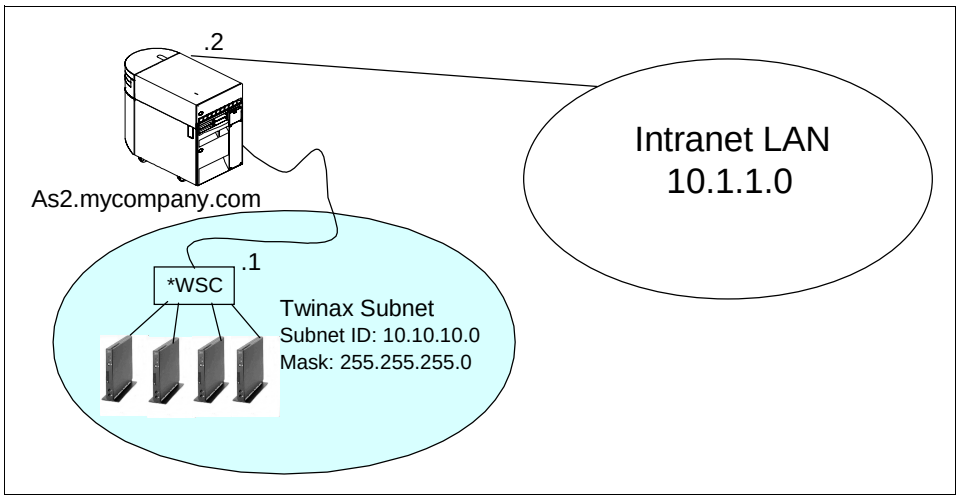


Figure 36. TCP/IP Network Topology for Basic IP over Twinax Scenario

5.4.6 Task Summary

The following tasks are required to implement this scenario:

1. Define a TCP/IP address range to use on the twinax subnet.
2. Configure and start the IBM Network Station.
3. Configure an AS/400 IP interface as determined by messages logged in the QSYSOPR message queue.

5.4.7 Defining a TCP/IP Address Range

For this scenario, any IP addresses can be assigned to the twinax subnet as the addresses are not externalized beyond the AS/400 server. The IP network associated with the AS/400 LAN card are not used. In this example, a network of 10.10.10.0 is used for the twinax subnet.

5.4.8 Configuring and Starting the IBM Network Station

It is assumed that you have cabled the twinax IBM Network Stations correctly. If you are replacing non-programmable terminals (NPT) with the twinax IBM Network Station, you should notice the twinax address and port that the original NPT was using. In most cases, you should be able to use the same port and address for the replacement IBM Network Station.

If you plan to use both NPTs and twinax IBM Network Stations on the same workstation controller, consider isolating the two types of terminals on different ports. With the system console located on port 0, the twinax IBM

Network Stations can be on port 1 or any other available port that does not have NPT's connected. This type of configuration is not mandatory but is suggested for performance reasons.

When a twinax IBM Network Station is powered on for the first time, it prompts you to specify the address to use for the port to which it is connected. *This is not the TCP/IP address***.** It is an address, from 0 through 6, to use on the workstation controller port to which the IBM Network Station is connected.

Follow these steps to configure the IBM Network Station to use over twinax:

1. Power on the IBM Network Station after it has been cabled correctly.
2. When prompted to do so, specify the local controller address to use (range is from 0 to 6).

   The IBM Network Station checks to see if any other device is using that address. If not, the particular address is accepted. If the address is in use by another device, a message *Station Address in Use* is displayed and another address must be chosen. Proceed with choosing another address (in the 0 to 6 range) until one is accepted.

   If you are not prompted for an address, then one has already been defined for the IBM Network Station. After the station powers up, bootup messages are logged. On a twinax IBM Network Station, one of those messages is *NS0065 Twinaxial station address...x,* where x is an address from 0 to 6.

   If an address has been defined, there may be other configuration parameters present on the Network Station. For a twinax IBM Network Station, limited configuration is required. If you suspect the Network Station has been configured before, we recommend that you *Reset NVRAM* with the following steps:

   a. Power up the Network Station.
   b. After *NS0500 Search for Host System* posts, press **ESC** to stop the start-up sequence.
   c. Press one of the following key sequences:
      - For 101/102 keyboards:

        Press and hold **Left Shift + Left Alt + Left Ctrl.** Press **F1.**
      - For 5250/3270 keyboards:

        Press and hold **Left Shift + Left Alt.** Press **F1**.
   d. Enter **NV** at the Boot Monitor command prompt (>) to access the NVRAM utility.

e. Enter **L** to reset the NVRAM.
f. Enter **S** save the defaults into NVRAM.
g. Enter **Y** to the question: *Are you sure?*
h. Enter **Q** to quit.
i. Power the IBM Network Station off and then on again. It starts with the factory settings and prompts you to input a station address.

If you only want to change the address, wait until the message *NS0500 Search for Host System* appears on the Network Station. Press **Esc** and select option 8 (Set Twinax Station Address), from the *IBM Network Station Setup Utility* menu.

3. The other change you must make, in the *IBM Network Station Setup Utility*, select option 3 (Set Network Parameters). Either one of the following settings works for this particular scenario:

   - For **NVRAM**, set all of the addresses to **0.0.0.0**.
   - For **Network**, set *DHCP IP Addressing Order* set to **Disabled** and *BOOTP IP Addressing Order* set to **1**.

   If you have chosen **Network,** ensure you have the *BOOTP* server started on the AS/400 system. To start the server, enter the following command:

   ```
   STRTCPSVR *BOOTP
   ```

5.4.9 Configuring an AS/400 IP Interface

After the necessary changes are made to the Network Station configuration using the IBM Network Station Setup Utility, reboot the Network Station. The boot up process logs messages *NS0010* through to *NS0500 Search for Host.*

When the *NS0500* message is logged, review the messages logged in the QSYSOPR message queue on the AS/400 system. Similar messages, as shown in Figure 37, should be posted.

```
                            Display Messages
                                                        System:   AS1
Queue . . . . . :   QSYSOPR               Program . . . . :   *DSPMSG
 Library . . . :     QSYS                  Library . . . :
Severity  . . . :   90                    Delivery  . . . :   *HOLD

Type reply (if required), press Enter.
  Automatic configuration created device description DSP02.
  DSP02 cannot connect.  TCP/IP interface not added for line QTDL824300.
  Line QTDL824300 varied on successfully.
  Controller QTDL8NET contacted on line QTDL824300.
```

Figure 37. Display of QSYSOPR Message Queue on AS/400 System

Note

If the message NS0500 is logged on the Network Station and there are no messages logged in QSYSOPR message queue, check the System Value QAUTOCFG using the AS/400 command DSPSYSVAL QAUTOCFG. If this value is set to OFF, change it to ON to connect and configure twinax IBM Network Stations to your AS/400 system.

The QHST log on the AS/400 system has additional messages logged, as shown in Figure 38.

```
 5769SS1 V4R3M0 980729                              History Log
 MSGID    SEV MSG TYPE
 CPC2622  00  COMPLETION   Description for device DSP02 created.
QSYSARB    QSYS       004352                   08/31/98 13:21:00
 CPC2605  00  COMPLETION  Vary on completed for device DSP02.
 QSYSARB    QSYS       004352                    08/31/98 13:21:00
CPC2630 00 COMPLETION Automatic configuration created device description DSP02.
QSYSARB    QSYS       004352                   08/31/98 13:21:00
 CPC2601  00  COMPLETION  Line description QTDL824300 created.
QLUS       QSYS       004357                   08/31/98 13:21:00
 CPC2623  00  COMPLETION  Description for controller QTDL8NET created.
QLUS       QSYS       004357                   08/31/98 13:21:00
 CPC2622  00  COMPLETION  Description for device QTDL8TCP created.
QLUS       QSYS       004357                   08/31/98 13:21:00
 CPC2607  00  COMPLETION  Vary on completed for line QTDL824300.
QLUS       QSYS       004357                   08/31/98 13:21:00
 CPC2609  00  COMPLETION  Vary on completed for controller QTDL8NET.
QLUS       QSYS       004357                   08/31/98 13:21:00
 CPF5909  00  INFO       Line QTDL824300 varied on successfully.
QSYSARB    QSYS       004352                   08/31/98 13:21:00
 CPIB461  60  INFO        DSP02 cannot connect.  TCP/IP interface not added for line
QTDL824300.
                  QSYSCOMM1  QSYS      004377               08/31/9813:21:00
 CPF5908  00  INFO      Controller QTDL8NET contacted on line QTDL824300.
                  QSYSARB    QSYS      004352               08/31/98 13:21:01
```

Figure 38. Display of QHST Log on the AS/400 System

The system automatically creates a QTDLC line, controller and device. Figure 39 on page 134 shows the configuration status display of these auto-created descriptors.

```
                      Work with Configuration Status                AS1
                                                          08/31/98  13:28:21
Position to  . . . . .               Starting characters
Type options, press Enter.
  1=Vary on   2=Vary off   5=Work with job   8=Work with description
  9=Display mode status    13=Work with APPN status...
Opt  Description       Status               -------------Job--------------
     QTDL824300        ACTIVE
       QTDL8NET        VARIED ON
         QTDL8TCP      VARIED OFF
```

Figure 39. Configuration Status Display of Automatically Created QTDL Descriptors

Figure 40 shows the detail of the twinaxial data link control line description.

```
                          Display Line Description                AS1
                                                          08/31/98  13:28:52
Line description . . . . . :   QTDL824300
Option . . . . . :   *BASIC
Category of line . . . . . :   *TDLC

Attached work station ctl  . . . . :   CTL01
Network controller . . . . . :   QTDL8NET
Online at IPL  . . . . . :   *NO
Text . . . . . :   CREATED BY AUTO-CONFIGURATION
```

Figure 40. QTDL824300 Line Description

The system also creates a display device; in this case it is DSP02.

This device is created underneath the workstation controller (CTL01 in this case) and its description is shown in Figure 41 on page 135.

```
                  Display Device Description                    Page     1
5769SS1 V4R3M0  980729                          AS1       08/31/98  13:28:37
 Device description . . . . . :   DEVD        DSP02
 Option . . . . . :   OPTION      *ALL
 Category of device . . . . . :               *DSP
 Device class . . . . . :   DEVCLS      *LCL
 Device type  . . . . . :   TYPE        5150
 Device model . . . . . :   MODEL       3
 Port number  . . . . . :   PORT        1
 Switch setting . . . . . :   SWTSET     0
 Online at IPL  . . . . . :   ONLINE     *YES
 Attached controller  . . . . . :   CTL         CTL01
 Keyboard language type . . . . . :   KBDTYPE    USB
 Print device . . . . . :   PRTDEV      *SYSVAL
 Output queue . . . . . :   OUTQ        *DEV
 Printer file . . . . . :   PRTFILE     QSYSPRT
   Library  . . . . . :                  *LIBL
 Workstation customizing object . . :   WSCST      *NONE
 Dependent location name  . . . . . :   DEPLOCNAME  *NONE

F3=Exit   F12=Cancel   F19=Left   F20=Right   F24=More keys
```

Figure 41. Automatically Created Device Type 5150 under CTL01

The next step is to create an IP interface for the automatically created TDLC line. For this scenario, the TDLC line is QTDL824300. Complete the following steps:

1. Type `ADDTCPIFC` on a command line and press **F4**.
2. Enter values for the *Internet address* (INTNETADR), *Line description* (LIND) and *Subnet mask* (SUBNETMASK) parameters. In our scenario, we used the values shown in Figure 42 on page 136.

```
                    Add TCP/IP Interface (ADDTCPIFC)

Type choices, press Enter.

Internet address . . . . . .   10.10.10.1
Line description . . . . . .   QTDL824300  Name, *LOOPBACK, *VIRTUALIP
Subnet mask  . . . . . . . .   255.255.255.0
Associated local interface . .  *NONE
Type of service  . . . . . .   *NORMAL       *MINDELAY, *MAXTHRPUT...
Maximum transmission unit  . .  *LIND         576-16388, *LIND
Autostart  . . . . . . . . .   *YES          *YES, *NO
PVC logical channel identifier                001-FFF
             + for more values
X.25 idle circuit timeout  . . .  60          1-600
X.25 maximum virtual circuits  .  64          0-64
X.25 DDN interface . . . . . .   *NO           *YES, *NO
TRLAN bit sequencing . . . . . .  *MSB         *MSB, *LSB

                                                                      Bottom
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

Figure 42. Adding IP Interface for QTDLC824300 Line Description

3. Start the interface that you have created. Type the command CFGTCP and then choose option **1** (Work with TCP/IP interfaces) as shown in Figure 43.

```
                        Work with TCP/IP Interfaces
                                                              System:   AS1
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display   9=Start   10=End

     Internet         Subnet             Line      Line
Opt  Address          Mask            Description  Type

     9.5.69.219       255.255.255.192  TRNLINE      *TRLAN
 9   10.10.10.1       255.255.255.0    QTDL824300   *TDLC
     127.0.0.1        255.0.0.0        *LOOPBACK    *NONE
```

Figure 43. Starting the Interface for the QTDLC824300 Line Description

4. Enter a **9** to start the 10.10.10.1 interface as shown in Figure 44 on page 137. Ensure that the status is *Active* by pressing **F11**.

   If you return to the Network Station, the boot process should be continuing. The TDLC component, on the AS/400 system, sends an initiation link to the IBM Network Station. This initiation link contains:

- The TCP/IP address (in this scenario 10.10.10.2) assigned to the Network Station.
- The IP address (in this scenario 10.10.10.1) for the Twinax interface.
- The Configuration Directory (in this scenario */QIBM/ProdData/NetworkStation/configs/*)

The IBM Network Station updates its own NVRAM settings with the Boot Host IP Address and Configuration Directory.

On the AS/400 system, the QTDLC line, controller and device are *ACTIVE*. The configuration display is shown in Figure 44.

```
                      Work with Configuration Status              AS1
                                                        08/31/98  13:30:05
Position to  . . . . .               Starting characters
Type options, press Enter.
  1=Vary on   2=Vary off   5=Work with job   8=Work with description
  9=Display mode status    13=Work with APPN status...
Opt  Description       Status               -------------Job--------------
     QTDL824300        ACTIVE
       QTDL8NET        ACTIVE
         QTDL8TCP      ACTIVE               QTCPIP      QTCP        004427
                                                                      Bottom
Parameters or command
===>
F3=Exit   F4=Prompt   F12=Cancel   F23=More options   F24=More keys
```

Figure 44. Configuration Status of QTDL824300 Line, Controller, and Device

The device description, DSP02, has also been updated to include the assigned IP address. A detailed description of this device is shown in Figure 45 on page 138.

```
                    Display Device Description                      Page     1
5769SS1 V4R3M0  980729                              AS1       08/31/98  13:30:24
 Device description . . . . . :   DEVD        DSP02
 Option . . . . . :   OPTION      *ALL
 Category of device . . . . . :               *DSP
 Device class . . . . . :   DEVCLS      *LCL
 Device type  . . . . . :   TYPE        5150
 Device model . . . . . :   MODEL       3
 Port number  . . . . . :   PORT        1
 Switch setting . . . . . :   SWTSET     0
 Internet address. . . . . :              10.10.10.2
 Online at IPL  . . . . . :   ONLINE      *YES
 Attached controller  . . . . . :   CTL         CTL01
 Keyboard language type . . . . . :   KBDTYPE     USB
 Print device . . . . . :   PRTDEV      *SYSVAL
 Output queue . . . . . :   OUTQ        *DEV
 Printer file . . . . . :   PRTFILE     QSYSPRT
   Library  . . . . . :                 *LIBL
 Workstation customizing object . . :   WSCST       *NONE
```

Figure 45. Updated 5150 Device Description

5. When the IBM Network Station was initially configured with the IBM Network Station Setup Utility, a value of either *NVRAM* or *Network* could be chosen (see Section 5.4.8, “Configuring and Starting the IBM Network Station” on page 130). If *Network* was chosen, then a BOOTP table entry was created on the AS/400 system. To view this, run the Work BOOTP Table (WRKBPTBL.) command. The resulting AS/400 display is shown in Figure 46.

```
                          Work with BOOTP Table
                                                          System:   AS1
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display

      Client
      Host                              MAC                IP
Opt   Name                              Address            Address

      DSP02_AS1.MYCOMPANY.COM           00.00.a7.02.38.d1  10.1.1.194
```

Figure 46. BOOTP Table Entry for Twinax IBM Network Station

To see a more detailed view of this bootup entry, type a **5** beside the entry. The full detail is then shown as in Figure 47 on page 139.

```
                        Display BOOTP Table Entry
                                                              System:   AS1
Network device:
  Client host name  . . :   DSP02_AS1.MYCOMPANY.COM
  MAC address . . . . . :   00.00.a7.02.38.d1
  IP address  . . . . . :   10.10.10.2
  Hardware type . . . . :   26
Network routing:
  Gateway IP address  . :
  Subnet mask . . . . . :
Boot:
  Type  . . . . . :   IBMNSM
  File name . . . . . :   kernel
  File path . . . . . :   /QIBM/ProdData/NetworkStation
Press Enter to continue.
```

Figure 47. Display of BOOTP Table Entry

5.4.10 Testing Connectivity

In this scenario, the IBM Network Station is able to start *only* 5250 sessions and access the Web server, using NC Navigator, on the serving AS/400 system.

The server AS/400 system, in this scenario, also has a LAN card installed. If the AS/400 system is configured as a mail server and has connectivity to the Internet, the IBM Network Station can use NC Navigator to send and receive Internet e-mail. For more information about using the IBM Network Station to access mail, please refer to Chapter 8, “Using a Network Station to Access Mail” on page 225.

5.4.11 Summary

This scenario installed a twinax subnet on an AS/400 system using an isolated network of 10.10.10.0. Minimum configuration was performed on each twinax IBM Network Station, including selecting a workstation address. With the help of messages logged on the AS/400 server, an IP interface was manually created for the automatically created QTDLC configuration. Activating this interface allowed the IBM Network Station to complete the boot up process.

Connectivity was tested by starting a 5250 session to the server AS/400 system and by accessing the IBM Network Station Manager program with NC Navigator.

5.5 Transparent Subnet Masking

In this scenario, we allow the twinax subnet access to the local LAN and beyond. With the introduction of *transparent subnet masking*, introduced in V4R2 of OS/400, an addressing scheme for the twinax subnet can be configured on the AS/400. This implementation allows IP over twinax devices to appear as though they were on the local network.

Transparent subnet masking uses different masks over the same network ID. This masking segments contiguous ranges of IP addresses together to use for either twinax subnets or for remote LANs attached to the AS/400 system. The transparency part comes into play when *Proxy ARP* is enabled, which happens automatically when the hosts on the network share the same network ID. In effect, the subnetting within your network is transparent because a router or gateway is *not* required to join the subnets.

Detailed information concerning *Proxy ARP* is beyond the scope of this redbook. Further information is found in the following sources:

- *AS/400 TCP/IP DNS and DHCP,* SG24-5147
- RFC 826 which discusses Address Resolution Protocol
- RFC 1027 which discusses Proxy ARP

The twinax subnet requires a contiguous range of TCP/IP addresses assigned to it. You *cannot* use any address at random from the pool and dynamically allocate an address to a device on the twinax subnet. The recommendation is that the maximum amount of TCP/IP addresses, which is 64, be assigned to the twinax subnet, if possible. This limit of 64 is actually imposed by the workstations controller. It is not a true limit because the workstation controller can only support up to 56 operational twinax devices.

By initially choosing to use the maximum number of TCP/IP addresses, there is flexibility later to add devices to the subnet without having to change the IP addressing scheme within the network. There are, however, smaller subnets that can be configured for your twinax IBM Network Stations. Detailed tables are included in *Appendix B* of the *IBM Network Station Manager Installation and Use,* SC41-0664. These tables outline exact ranges of IP Addresses used in each scenario, depending on the quantity of Network Stations needing support within the subnet.

Figure 48 on page 141 shows a simple example of a network that is using transparent subnet masking and *Proxy ARP.* All the networks and hosts are on the same TCP/IP network ID, 10.1.x.x.

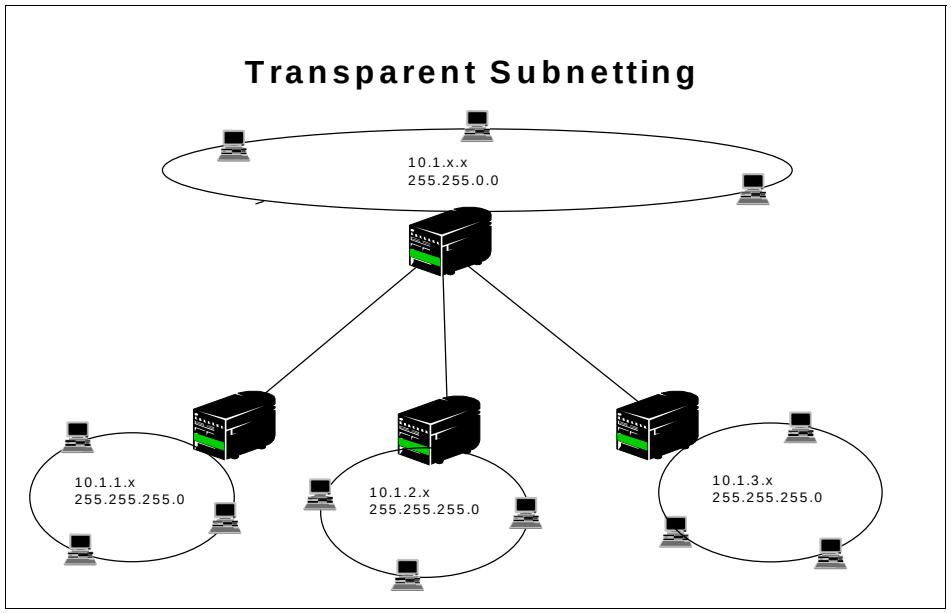


Figure 48. Transparent Subnetting Example

5.5.1 Twinax Transparent Subnetting Example

The twinax subnet requires a contiguous range of TCP/IP addresses defined and allocated. Figure 49 helps determine which mask to apply and what range of addresses you can use.

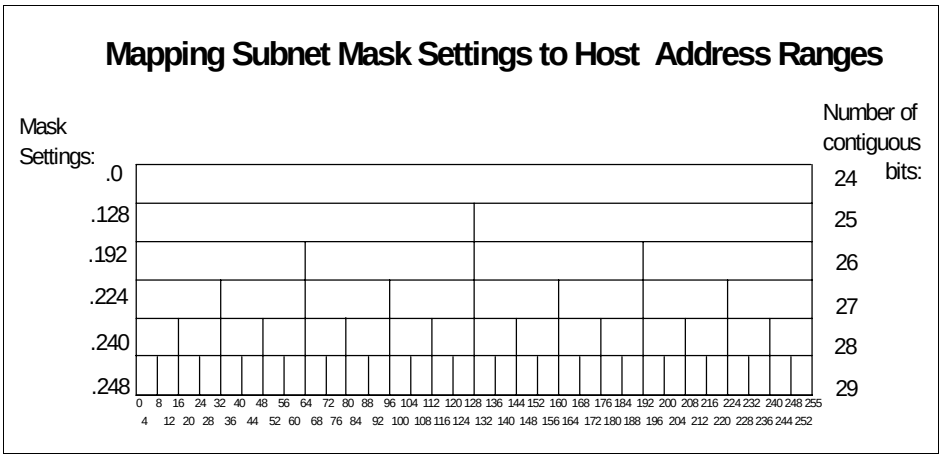


Figure 49. Subnet Mask Boundaries and Address Ranges

Looking at the Figure 49 on page 141, a mask of 128 in the last octet provides two address groups:

- .1 to .126
- .129 to .254

The subnet boundaries in both groups cannot be used. In this case, the addresses .0, .127, .128 and .255 cannot be used.

The same applies for a mask of 240. This mask gives you 16 groups of (16-2) contiguous addresses, remembering that the boundary addresses in each group, cannot be used.

For selecting twinax subnets, *only* consider mask settings of 248, 240, 224 and 192 because these subnets provide a number of IP addresses that are supported by the workstation controller. A mask of 128 or 0 can be assigned. However, many addresses in these groups cannot be used and hence are wasted. As previously mentioned, detailed tables outlining the combinations of subnet masks and groups of IP addresses can be found in *IBM Network Station Manager Installation and Use,* SC41-0664*.*

The next example uses a class **C** TCP/IP address that is divided into four different address groups. Three subnet groups, for three different TCP/IP over twinax networks, is assigned. A large group of addresses are allocated for the rest of the network.

Note

The following example does not follow the recommendation of allowing a maximum contiguous range of 64 TCP/IP addresses allocated to the twinax subnet. It is only intended to provide an example of transparent subnetting in a twinax environment. Unless you are limited, by your own network IP addressing scheme, to using such an example, allocate the maximum number of IP addresses to the twinax subnet.

Figure 50 on page 143 shows the Network Topology for this example and Figure 51 on page 143 shows the division of the address space 192.168.1.x.

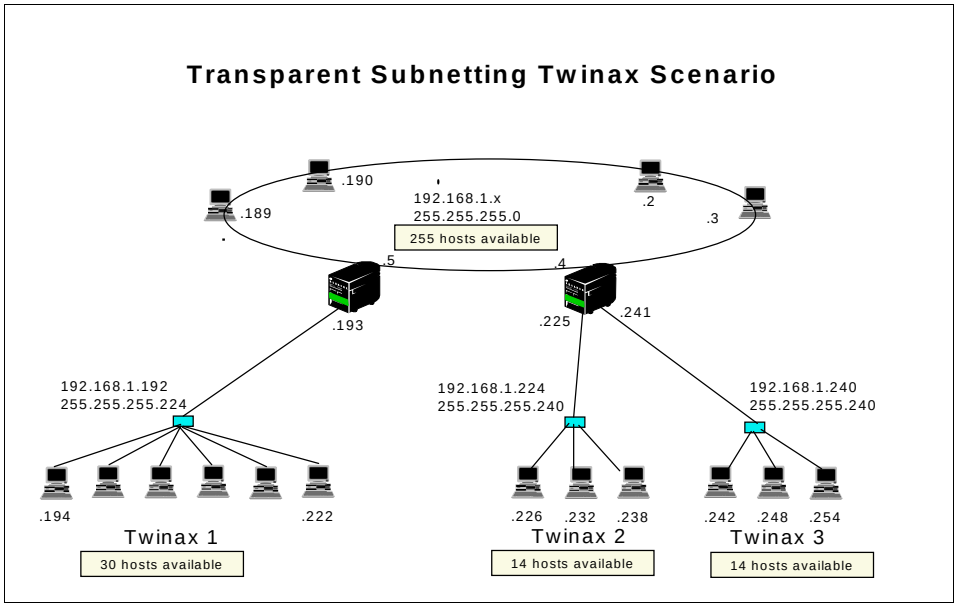


Figure 50. Transparent Subnetting Twinax Scenario with Class C TCP/IP Address

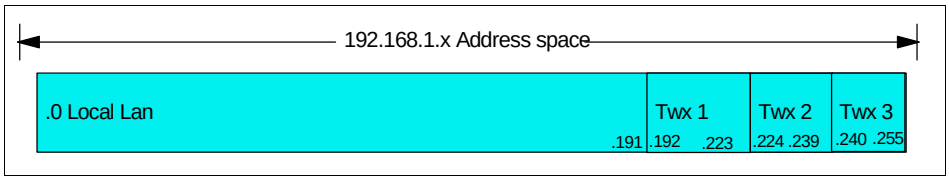


Figure 51. Transparent Subnetting Class C Address Example

The *Local LAN* has a network address of 192.168.1.0 and a mask of 255.255.255.0. This mask gives you the entire range of addresses to use in the last byte or octet of the address. As in our next scenario, we are using a DHCP configuration here to break up this entire range using masks. As shown in Figure 51, the *Local LAN* is configured to have a range of address from .1 to .191 (boundary address cannot be used). The remainder of the address space is reserved for different subnets.

The next group of addresses, *Twx1,* has a subnet address of 192.168.1.192 and a mask of 255.255.255.224. This mask gives you eight groups of 32 contiguous addresses (refer to Figure 17). Only the block containing the range of addresses from 193 through 222 is used. Remembering that

boundary addresses within a group cannot be used, the group of addresses for subnet *Twx1* is from 192.168.1.193 to 192.168.1.222.

The third group, *Twx2*, has a subnet address of 192.168.1.224 and a mask of 255.255.255.240. This mask gives you 16 groups of 16 contiguous IP addresses. The group of addresses that is defined, within DHCP, is from 192.168.1.225 to 192.168.1.238.

The last group, *Twx3,* has a subnet address of 192.168.1.240 and a mask of 255.255.255.240. This mask gives you 16 groups of 16 contiguous IP addresses.

The group of addresses that is defined, within DHCP, is from 192.168.1.241 to 192.168.1.254.

The last address in each of the subnets is reserved as the broadcast address.

5.6 Advanced IP over Twinax Scenario

This scenario extends the one in Section 5.4, “Basic IP over Twinax Scenario” on page 128. The twinax IBM Network Stations are again attached to the local workstation controller on the AS/400 system. However, these same Network Stations now have the capability of communicating with another host beyond the local workstation controller.

5.6.1 Scenario Overview

This scenario shows an example of a twinaxial Network Station subnet attached to an AS/400 system. This same AS/400 server has connectivity to a LAN.

There is a minimum configuration needed on the Network Stations and some TCP/IP configuration required on the AS/400 system. The twinaxial subnet is taken out of the main network of 10.1.1.0.

5.6.2 Scenario Objectives

The objectives of this scenario are to:

- Assign an IP subnet to be used by the twinax IBM Network Stations.
- Configure the twinax attached IBM Network Stations.
- Configure the AS/400 server to allow connectivity, for the attached IBM Network Stations, to other hosts on the LAN.

5.6.3 Scenario Advantages

The advantages of this scenario are:

- It is easy to connect twinax attached IBM Network Stations to an existing network.
- Minimal configuration required on the IBM Network Stations.
- The IBM Network Stations have access to hosts beyond the immediate AS/400 server.

5.6.4 Scenario Disadvantages

The disadvantage of this scenario is that an understanding of concepts, such as subnetting and Proxy ARP, may be required if the network has a somewhat restricted addressing scheme.

5.6.5 Scenario Network Configuration

Figure 52 shows the network topology used for this scenario. The twinax attached IBM Network Stations are connected to the As1 system. The IBM Network Stations are on their own subnet which is taken out of the address space 10.1.1.0.

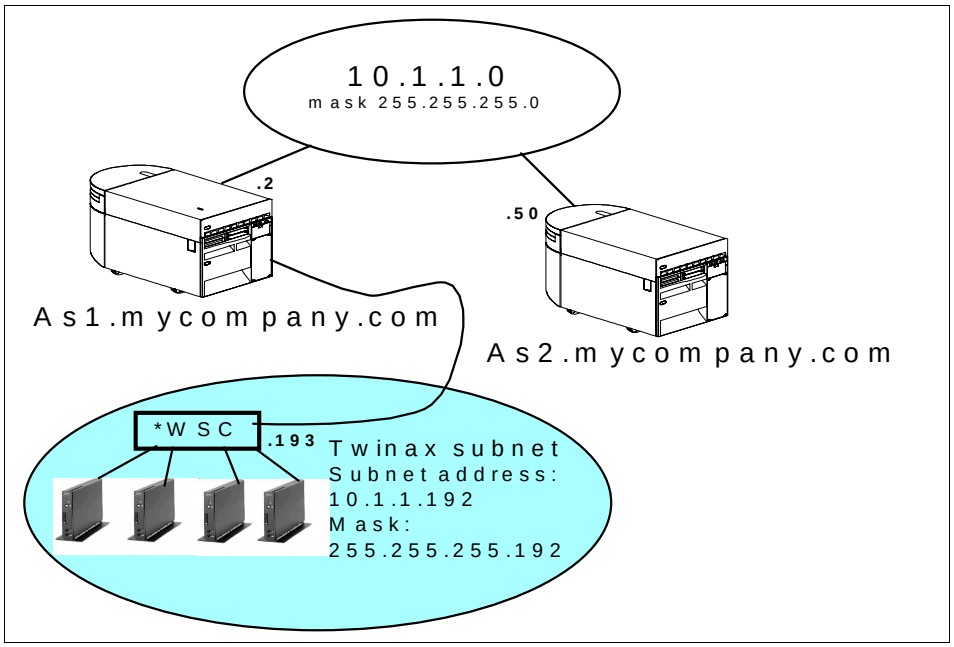


Figure 52. Network Topology for Advanced IP over Twinax Scenario

5.6.6 Task Summary

Note

Depending on the TCP/IP addressing scheme of your network, you must ensure that the address pool, which your are configuring for your twinax subnet, is not duplicated in another pool within the entire network.

If you have the ability in your network to allocate 64 IP addresses to the twinax subnet, you should do so and realize that some of the IP addresses will not be used. It becomes difficult, in networks other than class A, to reallocate and shift addressing schemes to gain another IP address to install additional twinax IBM Network Stations.

The following tasks are required to complete this scenario:

1. Plan and assign the TCP/IP addressing for the twinax subnet.
2. Configure and start the twinax IBM Network Station.
3. Configure an AS/400 IP interface as determined by messages logged in the QSYSOPR message queue.

5.6.7 Planning the TCP/IP Addressing Scheme

In a TCP/IP network, with a potential of multiple subnets and TCP/IP address ranges, it is imperative to carefully administer an addressing scheme for use by the twinax subnet.

For this scenario, Class A private IP addresses are used. These addresses cannot be routed through the internet. However, they provide good growth potential for your network in the future.

The network for this scenario is 10.1.1.0 with a subnet of 255.255.255.0. From this existing address space, we use a contiguous range of 64 IP addresses for use by the twinax IBM Network Stations. Applying a mask of 255.255.255.192 (which gives the maximum allowed TCP/IP address range of 64 that can be used on a twinax subnet) to this network of 10.1.1.0 gives us an address range of 10.1.1.192 to 10.1.1.255. Because this address range is a subset of the main network (10.1.1.0), Proxy ARP is enabled automatically.

The subnet boundaries in this group cannot be used. In this particular subnet, the addresses of 10.1.1.192 and 10.1.1.255 are not available, because 192 is used as the subnet address and 255 is used as the broadcast address. The

address of 10.1.1.193 is designated for the workstation controller (interface address).

Figure 53 provides a visual representation of the address space that is allocated to the twinax subnet.

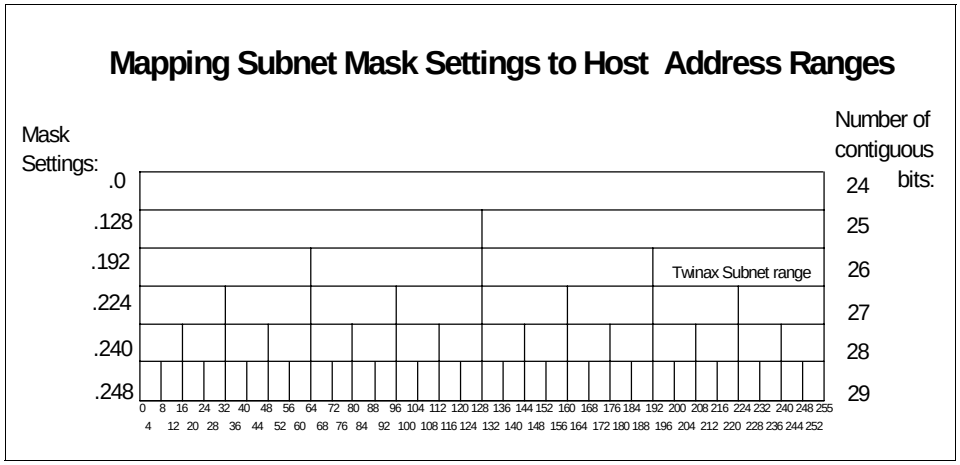


Figure 53. Applying Subnet Mask to Carve a Contiguous Range for Twinax Subnet

5.6.8 Configuring and Starting the IBM Network Station

For this scenario, the same steps as described in Section 5.4.8, “Configuring and Starting the IBM Network Station” on page 130 *should be followed.*

5.6.9 Configuring an AS/400 IP Interface

After the necessary changes are made to the Network Station configuration using the IBM Network Station Setup Utility, reboot the Network Station. The boot up process logs messages *NS0010* through *NS0500 Search for Host.*

When the *NS0500* message is logged, review the messages logged in the QSYSOPR message queue on the AS/400 system. Messages, similar to those in Figure 54 on page 148, are logged.

```
                              Display Messages
                                                          System:   AS1
Queue . . . . . :   QSYSOPR                 Program . . . . :   *DSPMSG
  Library . . . :     QSYS                    Library . . . :
Severity  . . . :   90                      Delivery  . . . :   *HOLD

Type reply (if required), press Enter.
  Automatic configuration created device description DSP02.
  Line QTDL827500 varied on successfully.
  DSP02 cannot connect.  TCP/IP interface not added for line QTDL827500.
  Controller QTDL8NET contacted on line QTDL827500.
```

Figure 54. Display of QSYSOPR Message Queue on AS/400 System

Note

If the message NS0500 is logged on the Network Station and there are no messages logged in QSYSOPR message queue, check the System Value QAUTOCFG using the AS/400 command DSPSYSVAL QAUTOCFG. If this value is set to *OFF*, change it to **ON** before connecting and configuring twinax IBM Network Stations to your AS/400 system.

The QHST log, on the AS/400 system, has additional messages logged. For a sample of these messages, refer to Figure 38 on page 133.

The system automatically creates a QTDLC line, controller and device as shown in Figure 55.

```
                     Work with Configuration Status              AS1
                                                        10/02/98  10:04:53
Position to  . . . . .              Starting characters

Type options, press Enter.
  1=Vary on   2=Vary off   5=Work with job   8=Work with description
  9=Display mode status    13=Work with APPN status...

Opt  Description       Status               -------------Job--------------
     QTDL827500        ACTIVE
       QTDL8NET        VARIED ON
         QTDL8TCP      VARIED OFF
```

Figure 55. Configuration Status Display of Automatically Created QTDL Descriptors

The display device created underneath the workstation controller (CTL01 in this case) is shown in Figure 56. This figure also shows the console, DSP01, for the AS/400 system.

```
                      Work with Configuration Status              AS1
                                                          10/02/98  10:06:17
Position to  . . . . .              Starting characters

Type options, press Enter.
  1=Vary on   2=Vary off   5=Work with job   8=Work with description
  9=Display mode status    13=Work with APPN status...

Opt  Description       Status               -------------Job--------------
     CTL01            ACTIVE
       DSP01          SIGNON DISPLAY
       DSP02          ACTIVE
```

Figure 56. Configuration Status Display of Automatically Created Display Device

The next step is to create an IP interface for the automatically created TDLC line. In Figure 55 on page 148, this line is QTDL827400. Complete the following steps:

1. Type `ADDTCPIFC` on any command line and press **F4**.
2. Enter values for the *Internet address* (INTNETADR), *Line description* (LIND), *Subnet mask* (SUBNETMASK) and *Associated local interface* (LCLIFC) parameters. The LCLIFC parameter is necessary in this scenario, to allow the IBM Network Stations to communicate beyond the workstation controller. The LCLIFC parameter associates the twinaxial interface with the LAN (token ring) interface. The values used in this scenario are shown in Figure 57 on page 150.

```
                    Add TCP/IP Interface (ADDTCPIFC)

Type choices, press Enter.

Internet address . . . . . .   10.1.1.193
Line description . . . . . .   QTDL827500    Name, *LOOPBACK, *VIRTUALIP
Subnet mask  . . . . . . . .   255.255.255.192
Associated local interface  10.1.1.2
Type of service  . . . . . .   *NORMAL       *MINDELAY, *MAXTHRPUT...
Maximum transmission unit  . . .  *LIND      576-16388, *LIND
Autostart  . . . . . . . . . .   *YES         *YES, *NO
PVC logical channel identifier                001-FFF
              + for more values
```

Figure 57. Adding IP Interface for QTDLC827500 Line Description

3. To start the interface that you have created, type `CFGTCP` on any command line and press **Enter**. Select option **1** (Work with TCP/IP interfaces) as shown in Figure 58. Enter an option **9** beside the 10.1.1.193 interface.

```
                        Work with TCP/IP Interfaces
                                                              System:   AS1
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display   9=Start   10=End

     Internet         Subnet             Line      Line
Opt  Address          Mask            Description  Type

     10.1.1.2         255.255.255.0    TRLAN2       *TRLAN
9    10.1.1.193       255.255.255.192  QTDL827500   *TDLC
     127.0.0.1        255.0.0.0        *LOOPBACK    *NONE
```

Figure 58. Starting the Interface for the QTDL827500 Line Description

4. Ensure that the status of the interface is *Active*. Press **F11** to see the status of the interfaces as shown in Figure 59 on page 151.

```
                        Work with TCP/IP Interfaces
                                                                  System:   AS1
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display   9=Start   10=End

     Internet         Subnet           Interface
Opt  Address          Mask             Status

     10.1.1.2         255.255.255.0    Active
     10.1.1.193       255.255.255.192  Active
     127.0.0.1        255.0.0.0        Active
```

Figure 59. TCP/IP Interface Status Display

If you return to the Network Station, the boot process should be continuing. The TDLC component, on the AS/400 system, sends an initiation link to the IBM Network Station. This initiation link contains:

- The assigned TCP/IP address (10.1.1.194 in this scenario) for the Network Station.
- The IP address (10.1.1.193 in this scenario) for the Twinax interface.
- The configuration directory (in this scenario */QIBM/ProdData/NetworkStation/configs/*).

The IBM Network Station updated its own NVRAM settings with the Boot Host IP Address (within the F3 display of the Setup Utility). Within the F5 display of the Setup Utility, the configuration directory is updated.

On the AS/400 system, the QTDLC line, controller and device are now ACTIVE as shown in Figure 60.

```
                      Work with Configuration Status              AS1
                                                          10/02/98  10:52:01
Position to  . . . . .              Starting characters

Type options, press Enter.
  1=Vary on   2=Vary off   5=Work with job   8=Work with description
  9=Display mode status    13=Work with APPN status...

Opt  Description       Status               -------------Job--------------
     QTDL827500        ACTIVE
       QTDL8NET        ACTIVE
         QTDL8TCP      ACTIVE               QTCPIP      QTCP        009024
```

Figure 60. Configuration Status of QTDL Descriptors

The display device, DSP02, is also updated to include the assigned IP address of 10.1.1.194. This is shown in Figure 61.

```
                        Display Device Description                AS1
                                                          10/02/98  10:54:54
Device description . . . . . :   DSP02
Option . . . . . :   *BASIC
Category of device . . . . . :   *DSP

Device class . . . . . :   *LCL
Device type  . . . . . :   5150
Device model . . . . . :   3
Port number  . . . . . :   1
Switch setting . . . . . :   0
Internet address . . . . . :   10.1.1.194
Online at IPL  . . . . . :   *YES
Attached controller  . . . . . :   CTL01
Keyboard language type . . . . . :   USB
```

Figure 61. Updated 5150 Device Description

5. When the IBM Network Station was initially configured with the IBM Network Station Setup Utility, a value of either *NVRAM* or *NETWORK* could be chosen (see Section 5.4.8, “Configuring and Starting the IBM Network Station” on page 130). If *Network* was chosen, then a BOOTP table entry was created on the AS/400 system. To view this, run the Work BOOTP Table (WRKBPTBL) command. The resulting AS/400 display is shown in Figure 62.

```
                          Work with BOOTP Table
                                                        System:   AS1
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display

      Client
      Host                              MAC               IP
Opt   Name                              Address           Address

      DSP02_AS1.MYCOMPANY.COM           00.00.a7.02.38.d1 10.1.1.194
```

Figure 62. BOOTP Table Entry for Twinax IBM Network Station

6. To see a more detailed view of this bootup entry, type a **5** beside the entry. The full detail is then shown as in Figure 63 on page 153.

```
                        Display BOOTP Table Entry
                                                              System:   AS1
Network device:
  Client host name  . . :   DSP02_AS1.MYCOMPANY.COM

  MAC address . . . . . :   00.00.a7.02.38.d1
  IP address  . . . . . :   10.1.1.194
  Hardware type . . . . :   26
Network routing:
  Gateway IP address  . :
  Subnet mask . . . . . :
Boot:
  Type  . . . . . :   IBMNSM
  File name . . . . . :   kernel

  File path . . . . . :   /QIBM/ProdData/NetworkStation
```

Figure 63. Display of BOOTP Table Entry

If *NVRAM* was chosen in the IBM Network Station Setup Utility when the Network Station was configured, a BOOTP table entry is *not* created.

5.6.10 Testing Connectivity

In this scenario, the IBM Network Station is able to access a host beyond the workstation controller. A 5250 TELNET session was started successfully to IP address 10.1.1.50 (AS2 system).

A 5250 TELNET session was also started successfully to the local system, AS1, at IP address 10.1.1.2.

Proxy ARP is also operational. A ping from the AS2 system to the twinax attached IBM Network Station, at address 10.1.1.194, was successful.

5.6.11 Summary

This scenario installed a twinax subnet on an AS/400 system using a subnet of the main 10.1.1.0 network. Minimal configuration was performed on each twinax IBM Network Station. An IP interface was manually created for the automatically created QTDL configuration, with the aid of messages logged on the AS/400 server system. This IP interface included an associated local interface (LCLIFC) parameter that associated the new twinax interface with the LAN interface on the AS/400 system. This allowed the IBM Network Station to connect to a system beyond the workstation controller.

Activating the new IP interface allowed the IBM Network Station to complete its boot up process. Connectivity was tested by starting a 5250 TELNET session to a remote AS/400 system, AS2.

5.7 Twinax IBM Network Station with Local DHCP Server Scenario

This scenario attaches the twinax IBM Network Stations to a local workstation controller on the AS/400 system. The local workstation controller is CTL01, which also supports the system console. DHCP is used to configure the workstation controller with an IP address and to provide the twinax IBM Network Stations with network start-up information.

A network addressing scheme, that enables Proxy ARP, is implemented. This will allow the twinax IBM Network Stations to see, and be seen, across the network.

5.7.1 Scenario Overview

This scenario shows an example of a twinaxial Network Station subnet. The AS/400 server has connectivity to a token ring LAN.

There is minimal configuration needed on the Network Stations. DHCP configuration is required on the AS/400 server.

5.7.2 Scenario Objectives

The objectives for this scenario are to:

- Configure the DHCP server, system As1, to support the locally attached twinax IBM Network Stations.
- Configure and start the twinax IBM Network Stations.
- Ensure LAN connectivity across the network.

5.7.3 Scenario Advantages

The advantages of this scenario include:

- Easy to connect twinax-attached IBM Network Stations to an existing network
- Easier to configure DHCP to support the twinax attached IBM Network Stations
- Automatic routing of datagrams from the twinax subnet to the attached LAN and, vice versa, when using Proxy ARP

5.7.4 Scenario Disadvantages

The disadvantage of this scenario is that an understanding of concepts, such as subnetting and Proxy ARP, may be required if the network has a somewhat restricted addressing scheme.

5.7.5 Scenario Network Configuration

Figure 64 shows the network topology used for this scenario. The twinax attached IBM Network Stations are connected to the DHCP server, As1. The IBM Network Stations receive their start-up information from the As1 system. The IBM Network Stations are on their own subnet which is taken out of the address space 10.1.1.0.

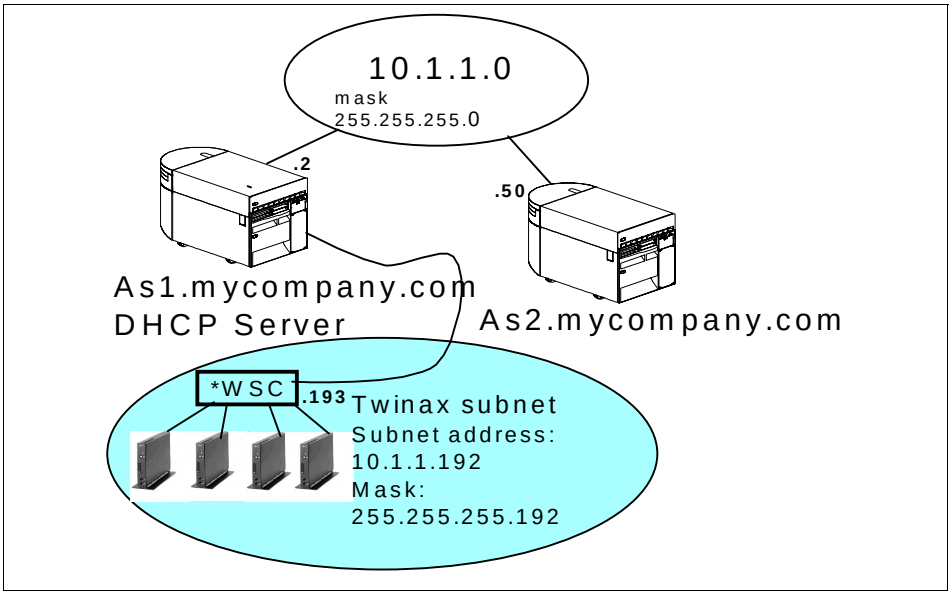


Figure 64. Network Topology for Local DHCP Server Scenario

5.7.6 Task Summary

Note

Depending on the TCP/IP addressing scheme of your network, you must ensure that the address pool, that you use for your twinax subnet, is not duplicated in a pool on another DHCP server within the same network. Operations Navigator DHCP server configuration does not allow you to create duplicate IP addresses in two subnets on the *same* DHCP server.

If you have the ability, in your network, to allocate 64 IP addresses to the twinax subnet, you should do so. Realize that some of the IP addresses will not be used. It becomes difficult, in networks other than class A, to reallocate and shift addressing schemes to gain another IP address to install additional twinax IBM Network Stations.

The following tasks are required to complete this scenario:

1. Plan and assign the TCP/IP addressing for the twinax subnet.
2. Configure the DHCP server for twinax support.
3. Configure and start the twinax IBM Network Station.
4. Test connectivity.

5.7.7 Planning the TCP/IP Addressing Scheme

In a TCP/IP network, with a potential of multiple subnets and TCP/IP address ranges, it is imperative to carefully administer an addressing scheme for use by the twinax subnet.

For this scenario, Class A private IP addresses are used. These addresses cannot be routed through the internet. However, they do provide good growth potential for your network in the future.

The network for this scenario is 10.1.1.0 with a subnet of 255.255.255.0. From this existing address space, we use a contiguous range of 64 IP addresses for use by the twinax IBM Network Stations. Applying a mask of 255.255.255.192 (which gives the maximum allowed TCP/IP address range of 64 that can be used on a twinax subnet) to this network of 10.1.1.0 gives us an address range of 10.1.1.192 to 10.1.1.255. Because this address range is a subset of the main network (10.1.1.0), Proxy ARP is enabled automatically.

Refer to Figure 65 on page 157 for a visual representation of the address space that is allocated to the twinax subnet.

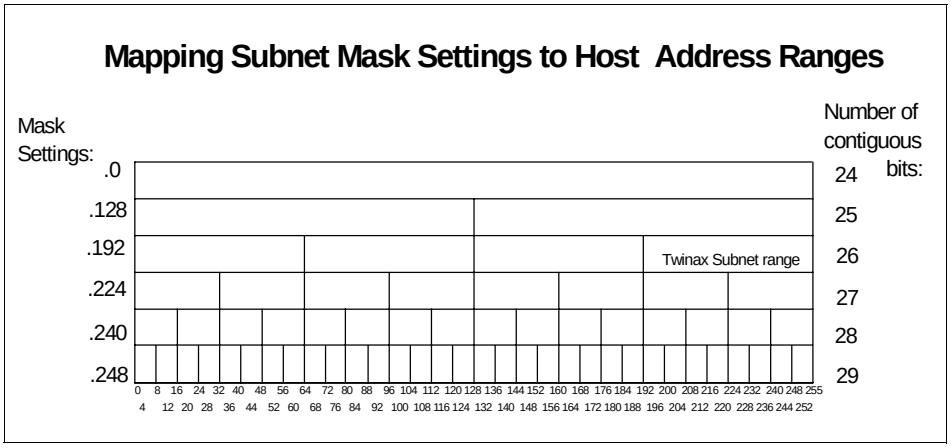


Figure 65. Applying Subnet Mask to Carve a Contiguous Range for Twinax Subnet

5.7.8 Configuring the DHCP Server As1 for Twinax Support

Note

The Operations Navigator displays shown in this section were captured from a PC running IBM AS/400 Client Access for Windows 95/NT Version 3 Release 2 Modification Level 0.

Operations Navigator DHCP configuration is twinax aware. If you have planned the IP addresses to use on the twinax subnet, the configuration of the DHCP server is straightforward.

On the DHCP server (As1 system), which has the IBM Network Stations attached using twinax to workstation controller CTL01, follow these steps to configure DHCP support for TCP/IP over twinax:

1. Start the AS/400 Operations Navigator.
2. Click **As1** to select the system. The display shown in Figure 66 on page 158 appears.

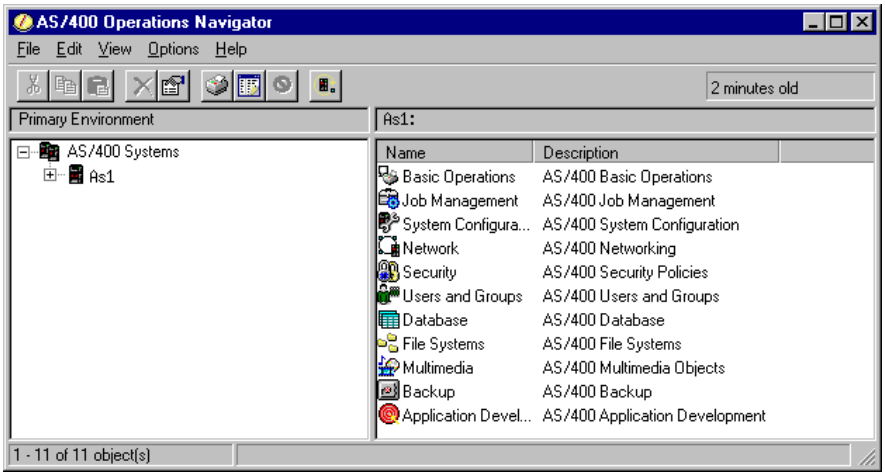


Figure 66. AS/400 Operations Navigator - Configure DHCP Server

3. Double-click **Network**. This display in Figure 67 is shown.

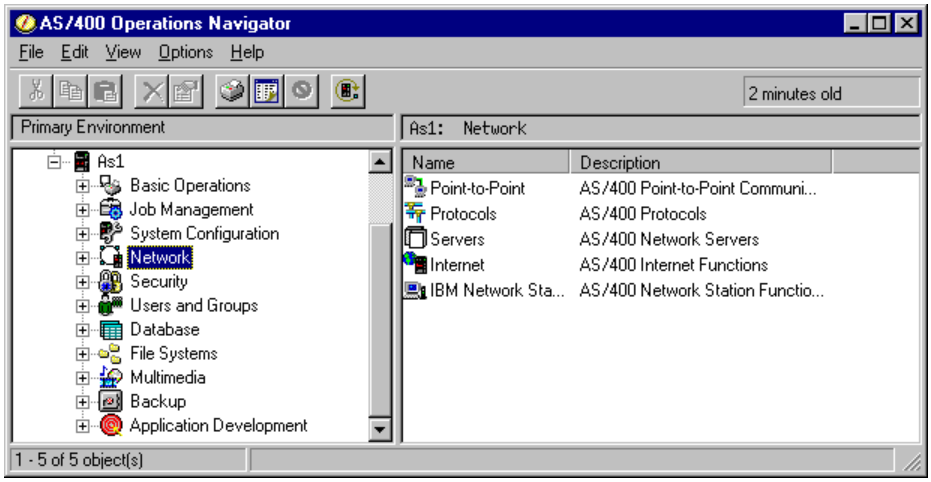


Figure 67. AS/400 Operations Navigator - Selecting Network

4. Double-click **Servers**. The display Figure 68 is shown.

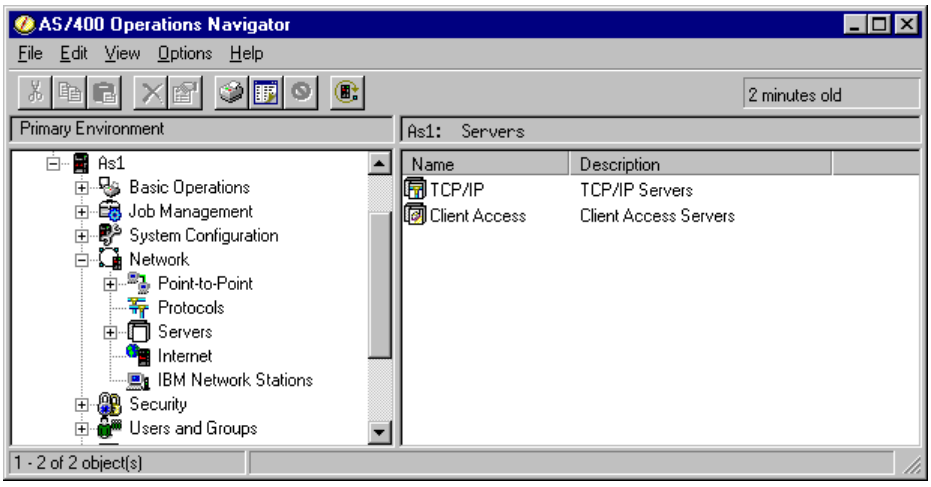


Figure 68. AS/400 Operations Navigator - Selecting Network Servers

5. Double click **TCP/IP**. The display Figure 69 is shown.

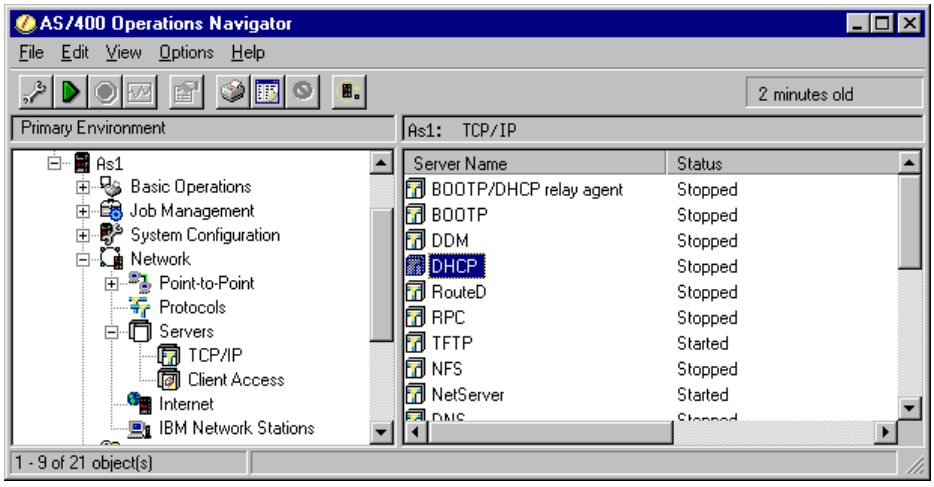


Figure 69. AS/400 Operations Navigator - Selecting TCP/IP Servers

6. Double-click **DHCP.** This shows the DHCP Server Configuration display (see Figure 70 on page 160). Ensure that *Global* is highlighted.

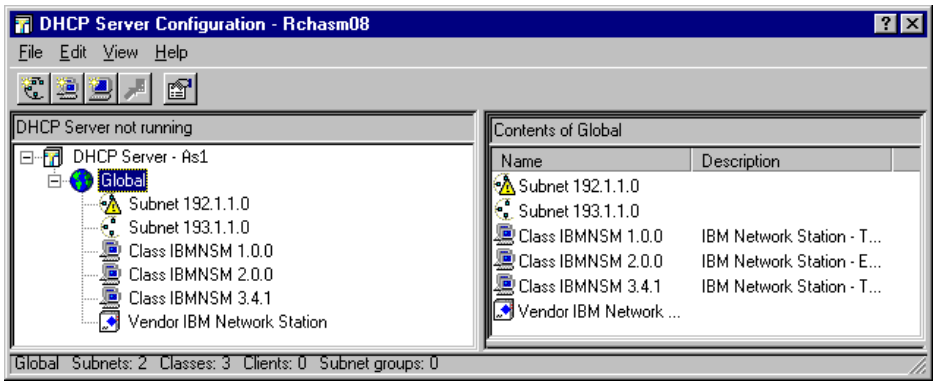


Figure 70. AS/400 Operations Navigator - DHCP Configuration

7. Right-click the mouse on **Global**. Select **New-Subnet Advanced**.

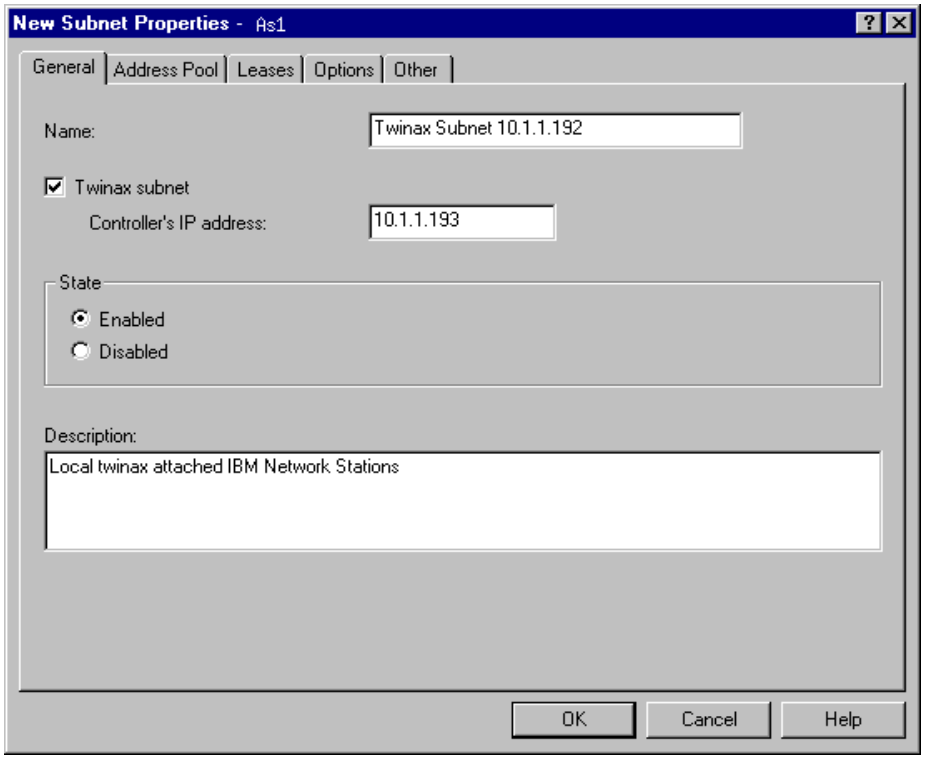


Figure 71. DHCP Server Configuration Twinax Subnet

8. As shown in Figure 71 on page 160, select the **General** tab. Specify **Twinax Subnet 10.1.1.192** in the *Name* field. Specify a network ID to make it easier to distinguish the twinax subnet from the other subnets.
9. Check *Twinax subnet* to enable it.
10. Specify the IP address of the workstation controller in the field *Controller's IP address*. The first usable address of the allocated subnet is used. In this scenario the address is **10.1.1.193**.
11. Specify a short description in the *Description* field, as shown in Figure 71.
12. Click the **Address Pool** tab.

    In Figure 72 on page 162, notice that the DHCP configuration dialog has already calculated the correct IP address range. The dialog calculated this range based on the network ID and the IP address that you supplied for the twinax workstation controller. You can change the subnet mask on this dialog and have the DHCP configuration GUI calculate the new values for you. However, remember, in this scenario, that the maximum number of addresses that can be allocated to the twinax subnet is 64.

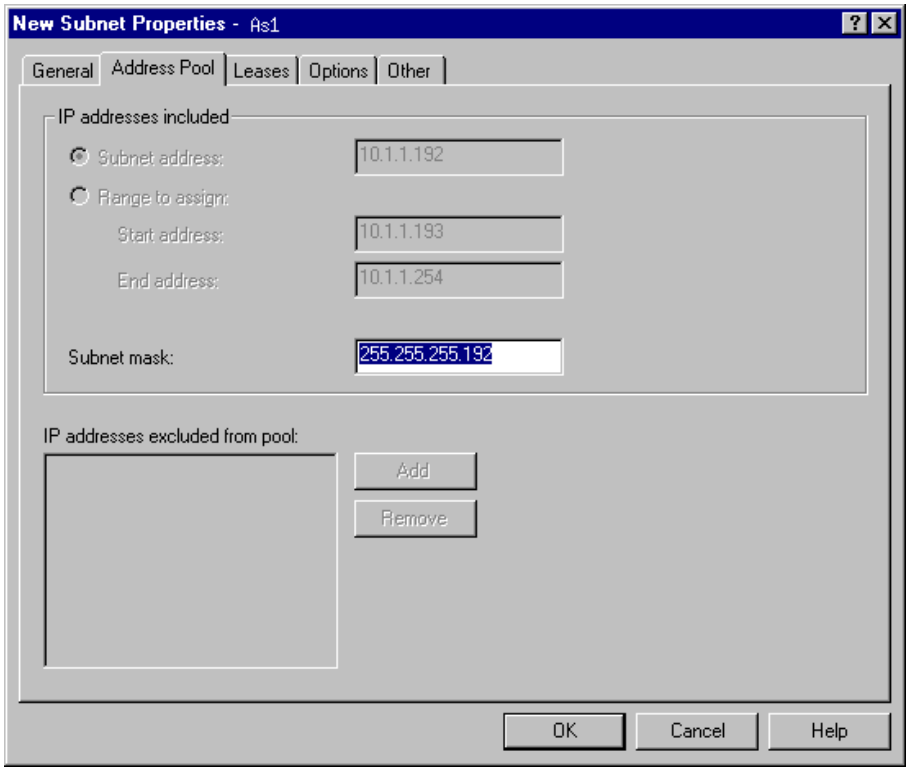


Figure 72. DHCP Twinax Address Pool Range

Tip

You do not need to exclude the workstation controller IP address from the range as seen in Figure 72. The configuration excludes this address automatically.

13. Click the **Leases** tab.
14. Set the lease time to **Never expire**.

15. Click the **Options** tab, as shown Figure 73 on page 163.
16. Add the options for the DHCP server-to-server shown in Table 18 to the twinax IBM Network Stations.

Table 18. Options for DCHP Server-to-Server

Option	Value
1 Subnet Mask	255.255.255.192
3 Router	10.1.1.193 (the WSC is the first hop attached device)
66 Server name	10.1.1.193
67 Boot file name	QIBM/ProdData/NetworkStation/kernel
Note: You should not need to add option 67; it is included in the twinax IBM Network Station class, IBMNSM3.4.1.	

The options, when added, appear as shown in Figure 73.

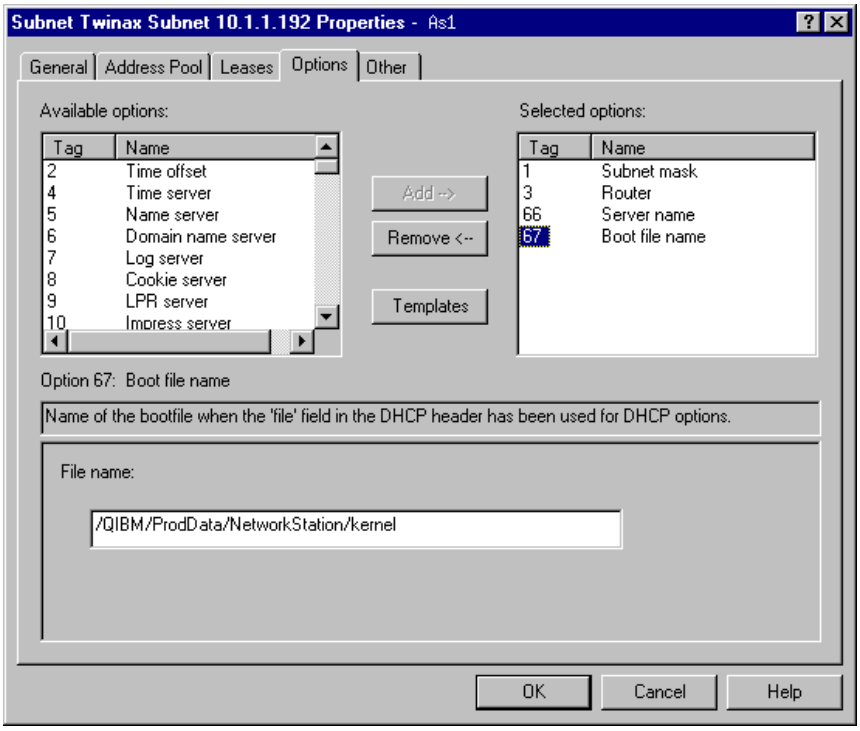


Figure 73. Twinax Attached DHCP Options Configuration

17. Click **OK**.

18. Close the DHCP configuration window. If the DHCP server is running, you are asked to save the changes you made. Click **YES**. If the DHCP server is not running, the configuration GUI closes and returns you back to the TCP/IP server display.

19. Start the DHCP server by right clicking on **DHCP** and select **Start**. If the DHCP server starts successfully, the *status* is updated as shown in Figure 74 on page 164.

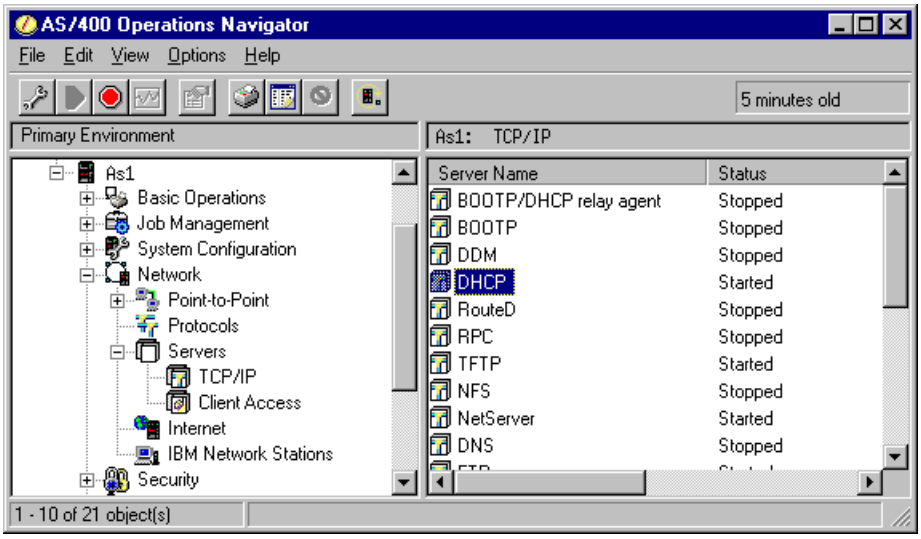


Figure 74. AS/400 Operations Navigator - TCP/IP Server Status

Note

If the DHCP Server fails to start, ensure that the BOOTP server is stopped. You cannot run both the BOOTP and DHCP server on the system at the same time.

5.7.9 Configuring and Starting the IBM Network Station

It is assumed that you have cabled the twinax IBM Network Stations correctly. If you are replacing non-programmable terminals (NPTs) with the twinax IBM Network Station, notice the twinax address and port that the old NPT was

using. In most cases, you should be able to use the same port and address for the replacement IBM Network Station.

When a twinax IBM Network Station is powered on for the first time, it prompts you to specify the address to use for the port to which it is connected. *This is not the TCP/IP address.* It is an address, from 0 through 6, to use on the workstation controller port to which the IBM Network Station is connected.

Use the following steps to configure the IBM Network Station to use over twinax:

1. Power on the IBM Network Station after it has been cabled correctly.
2. When prompted to do so, specify the local controller address to use (range is from 0 to 6).

   The IBM Network Station checks to see if any other device is using that address. If not, the particular address is accepted. If the address is in use by another device, the message, *Station Address in Use,* is shown and another address must be chosen. Proceed with choosing another address (in the 0 to 6 range) until one is accepted.

   If you are not prompted for an address, then one has already been defined for the IBM Network Station. After the Network Station powers up, bootup messages are logged. On a twinax IBM Network Station, one of those messages is *NS0065 Twinaxial station address...x,* where x is an address from 0 through 6.

   If an address is defined, there may be other configuration parameters present on the Network Station. For a twinax IBM Network Station, minimal configuration is required. If you suspect the Network Station has been configured before, we recommend that you reset *NVRAM* using the following steps:

   a. Power up the Network Station.
   b. After *NS0500 Search for Host System* is shown, press **ESC** to stop the start-up sequence.
   c. Press one of the following key sequences:

      - For 101/102 keyboards:

        Press and hold **Left Shift + Left Alt + Left Ctrl.** Press **F1.**

      - For 5250/3270 keyboards:

        Press and hold **Left Shift + Left Alt.** Press **F1**.

   d. Enter **NV** at the Boot Monitor command prompt (>) to access the NVRAM utility.

e. Enter **L** to reset the NVRAM.
f. Enter **S** save the defaults into NVRAM.
g. Enter **Y** to the question: *Are you sure?*
h. Enter **Q** to quit.
i. Power the IBM Network Station off and then on again. It starts with the factory settings and prompts you to input a station address.

If you only want to change the address, wait until message *NS0500 Search for Host System* appears on the Network Station. Press **ESC** and select option **8** (Set Twinax Station Address), from the IBM Network Station Setup Utility menu.

3. In the IBM Network Station Setup Utility, select option **3** (Set Network Parameters). Ensure the following settings:
   - For **NVRAM**, set all of the addresses set to 0.0.0.0.
   - For Network, set *DHCP IP Addressing Order* to **1.** Set *BOOTP IP Addressing Order* to **Disabled**.

   When these values are set, ensure that *Network* is highlighted.

5.7.9.1 Start-up Sequence

When the first IP over twinax IBM Network Station starts, OS/400 checks to see if a TCP/IP interface of type *TDLC exists. If not, the workstation controller calls the program QSYS/QTODDTWX to query the DHCP server configuration file (*dhcpsd.cfg)* for a TCP/IP address and mask to use.

The system automatically builds a QTDLxxxxxx line, controller, and device. A device type of 5150 is created underneath the workstation controller description for each Network Station. Figure 75 on page 167 shows the QTDL objects created by the automatic configuration.

Tip

If the IBM Network Station displays the NS0500 message and no further messages are logged, ensure that the system value *QAUTOCFG* is turned on.

```
                    Work with Configuration Status              AS1
                                                        09/16/98  16:06:25
Position to  . . . . .              Starting characters

Type options, press Enter.
  1=Vary on   2=Vary off   5=Work with job   8=Work with description
  9=Display mode status    13=Work with APPN status...

Opt  Description       Status               -------------Job--------------
     QTDL825900        ACTIVE
       QTDL8NET        ACTIVE
         QTDL8TCP      ACTIVE               QTCPIP      QTCP        006736
```

Figure 75. QTDLxxxxxx Line, Controller, and Device Configuration Status

Figure 76 shows the twinaxial data link control line description.

```
                        Display Line Description                AS1
                                                        09/16/98  16:26:08
 Line description . . . . . . . . . :   QTDL825900
 Option . . . . . . . . . . . . . . :   *BASIC
 Category of line . . . . . . . . . :   *TDLC

 Attached work station ctl  . . . . :   CTL01
 Network controller . . . . . . . . :   QTDL8NET
 Online at IPL  . . . . . . . . . . :   *NO
 Text . . . . . . . . . . . . . . . :   CREATED BY AUTO-CONFIGURATION
```

Figure 76. QTDLxxxxxx Line Description

The device created underneath the workstation controller, CTL01 in our scenario, is shown in Figure 77 on page 168. This device description also shows the IP address assigned to this particular IBM Network Station.

```
                        Display Device Description              AS1
                                                          09/16/98  16:28:16
Device description . . . . . :   DSP02
Option . . . . . :   *BASIC
Category of device . . . . . :   *DSP

Device class . . . . . :   *LCL
Device type  . . . . . :   5150
Device model . . . . . :   3
Port number  . . . . . :   1
Switch setting . . . . . :   0
Internet address . . . . . :   10.1.1.194
Online at IPL  . . . . . :   *YES
Attached controller  . . . . . :   CTL01
Keyboard language type . . . . . :   USB
Print device . . . . . :   *SYSVAL
Output queue . . . . . :   *DEV
```

Figure 77. Device Type 5150 under CTL01

The system automatically creates a TCP/IP interface for the workstation controller with a link type of *TDLC. This interface contains a parameter that allows the use of Proxy ARP. This parameter is called the *Associated local interface* (LCLIFC). Its value *must* be the LAN interface of the AS/400 system where the twinax workstation controller resides. In our scenario, this LAN interface has an IP address of 10.1.1.2.

Figure 78 shows the interface descriptor when it is first created by the system. Notice the LCLIFC parameter defaults to *NONE.

```
                        Display TCP/IP Interface
                                                          System:   AS1
Internet address . . . . . . . . . . . . . . . :   10.1.1.193
Subnet mask  . . . . . . . . . . . . . . . . . :   255.255.255.192
Line description . . . . . . . . . . . . . . . :   QTDL825900
Line type  . . . . . . . . . . . . . . . . . . :   *TDLC
Associated local interface. . . . . . . . . :   *NONE
Interface status . . . . . . . . . . . . . . . :   Active
Type of service  . . . . . . . . . . . . . . . :   *NORMAL
Maximum transmission unit  . . . . . . . . . . :   *LIND
Automatic start  . . . . . . . . . . . . . . . :   *YES
```

Figure 78. TCP/IP Interface for the Local Workstation Controller

For the twinax IBM Network Station to see and be seen across the network, the LAN interface must be *manually* added in the LCLIFC parameter of the TCP/IP TDLC interface.

To add the LAN interface, complete the following steps:

1. From an AS/400 session, enter `CFGTCP` on any command line.
2. Select option **1** (Work with interfaces).
3. To end the TDLC interface, select option **10**.
4. Select option **2** to change the interface. In this scenario, the 10.1.1.193 interface is ended.
5. Input the value **10.1.1.2** into the *Associated local interface* parameter and press **Enter**. A display of the Interface description is shown in Figure 79 on page 170.
6. Start the TDLC interface.
7. At this point, the twinax IBM Network Stations should show the initial login display. Because of the change we made to the IP interface, reboot the Network Stations.

```
                        Display TCP/IP Interface
                                                              System:   RCHASM08
Internet address . . . . . . . . . . . . . . . :   10.1.1.193
Subnet mask  . . . . . . . . . . . . . . . . . :   255.255.255.192
Line description . . . . . . . . . . . . . . . :   QTDL825900
Line type  . . . . . . . . . . . . . . . . . . :   *TDLC
Associated local interface. . . . . . . . . :   10.1.1.2
Interface status . . . . . . . . . . . . . . . :   Active
Type of service  . . . . . . . . . . . . . . . :   *NORMAL
Maximum transmission unit  . . . . . . . . . . :   *LIND
Automatic start  . . . . . . . . . . . . . . . :   *YES
```

Figure 79. TCP/IP Interface Updated with an Associated Local Interface Value

Note

At the time of writing, there was a documented problem with the LCLIFC parameter within the TCP/IP Interface. After entering an IP address within this parameter, a display of the interface still showed the previous value (for example *NONE). The user must do a refresh (F5) on the *Work with TCP/IP Interface* display. A subsequent display of the interface then shows the updated *Associated local interface* parameter.

A check of the configuration, within the IBM Network Station Setup Utility shows:

- The Twinax interfaces IP address (in this scenario 10.1.1.193) shown under NVRAM settings - Boot Host IP Address in F3=Set Network Parameters.
- The configuration directory (in this scenario */QIBM/ProdData/NetworkStation/configs/*) shown under the Configuration Directory in F5=Set Configuration Parameters.

5.7.10 Testing Connectivity

The DHCP server is configured for the twinax environment and a twinax IBM Network Station is started, after the *Associated local interface* parameter has been updated in the interface of type *TDLC. Now, you can test for connectivity across the network.

To prove that the IBM Network Station sees beyond the local workstation controller, start a 5250 TELNET session to *As2.mycompany.com,* which has an IP address of 10.1.1.50. The attempt was successful.

A test of Proxy ARP is to ping the twinax attached IBM Network Station from a remote host. From *As2.mycompany.com*, a ping is sent to address 10.1.1.194. The attempt was successful.

5.7.11 Summary

This scenario installed a twinax subnet on a DHCP server. The twinax address range, that was used, is a subset of the address space 10.1.1.x. A range of 64 IP addresses was allocated for the twinax subnet.

A DHCP server configuration was built for the twinax subnet. When the twinax IBM Network Stations were powered on, the AS/400 system automatically built the necessary TDLC configurations and a TCP/IP interface for the workstation controller. A manual change was required on this TCP/IP interface and the IBM Network Stations required a reboot.

After the IBM Network Station was restarted, connectivity was tested to the rest of the network by starting a 5250 TELNET session to a remote host. This same remote host successfully sent a ping request to the IBM Network Station.

5.8 Twinax IBM Network Station with a Remote DHCP Server Scenario

This scenario shows how to configure and use a remote DHCP server to supply network information to twinax connected IBM Network Stations.

It is not necessary to use the same system, to which the twinax attached IBM Network Stations are connected, as your DHCP server. You can utilize another DHCP server in your network.

5.8.1 Scenario Overview

In this scenario, there are twinax attached IBM Network Stations connected to a local AS/400 system. Although this AS/400 system is not acting as a DHCP server, it is serving as a BOOTP/DHCP Relay Agent.

Locally attached IP over twinax devices have their DHCPDISCOVER messages forwarded to a DHCP server that is running on a different AS/400 system. This is done to obtain a network address and start-up information that is required for boot up.

Figure 80 on page 172 shows the logical network topology that is used in this scenario. The twinax IBM Network Stations are attached to the

BOOTP/DHCP Relay Agent server which forwards all DHCP broadcasts, originating from the twinax subnet to the primary DHCP server, system As2.

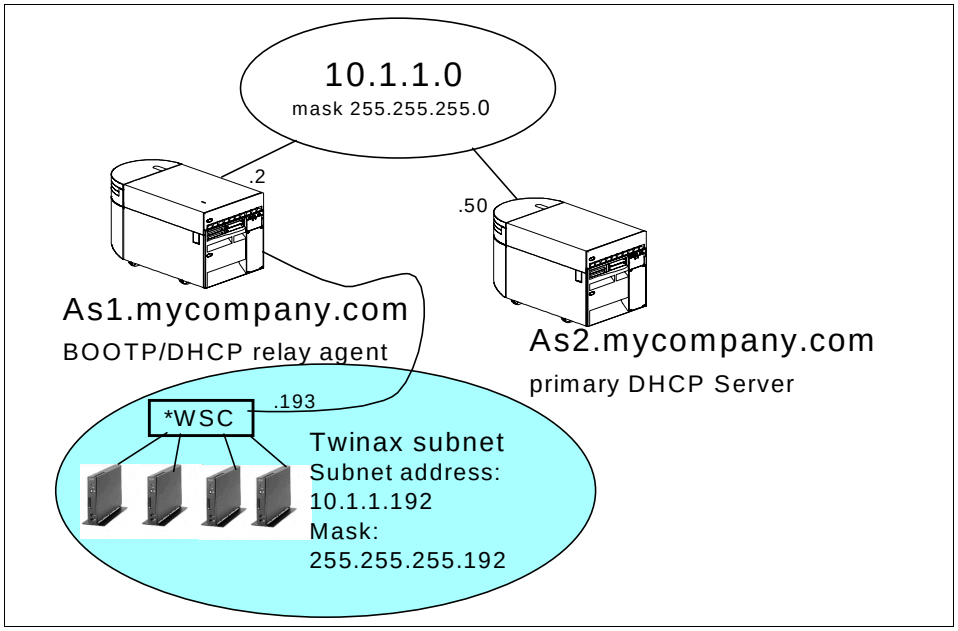


Figure 80. Using Remote DHCP Server to Configure Twinax IBM Network Stations

5.8.1.1 Scenario Objectives

This scenario's objective is to use one primary DHCP server to supply the necessary network information to remote twinax attached devices. This means that you do not have to run a DHCP server on every AS/400 system that has twinax attached IBM Network Stations.

5.8.1.2 Scenario Advantages

The advantage of this scenario is that you only need one DHCP server in your network to support twinax attached IBM Network Stations.

5.8.1.3 Scenario Disadvantages

The disadvantage of this scenario is that an understanding of concepts, such as subnetting and Proxy ARP, may be required if the network has a somewhat restricted addressing scheme.

5.8.2 Task Summary

In these setup steps, the assumption is made that the IBM Network Station is cabled correctly and that a local twinax address is defined on the IBM

Network Station. It is also assumed that the IBM Network Station can start as a DHCP client. The following tasks start from the point when the first IBM Network Station is ready to be powered on:

1. Configure the local AS/400 DHCP configuration file on *As1.mycompany.com.*
2. Power on the IBM Network Station. This automatically builds the TCP/IP interface on the local AS/400 system for the workstation controller. After this completes, the IBM Network Station can be powered off.
3. Manually change the auto created TCP/IP interface on the As1 system.
4. Configure and start the BOOTP/DHCP Relay Agent on the local AS/400 system *As1.mycompany.com*.
5. Change the DHCP configuration for the pool of addresses from 10.1.1.1 through 10.1.1.254 on the AS/400 system *As2.mycompany.com.*
6. Configure an address pool, on the As2 system, for the twinax subnet on the remote AS/400 system *As1.mycompany.com.*
7. Start the IBM Network Station.

5.8.3 Configuring the Local DHCP Configuration File on As1

There is a requirement to build a DHCP server configuration file (*dhcpsd.cfg*) on the system to which the twinax subnet is directly attached. You do *not* start the DHCP server on this AS/400 system. However, the configuration *must exist.* When the first IBM Network Station is powered on, the workstation controller calls the program QSYS/QTODDTWX. This program queries the DHCP configuration file for its IP address and mask.

Refer to Section 5.7.8, “Configuring the DHCP Server As1 for Twinax Support” on page 157 and follow steps 1 through 12. This scenario uses the same IP addressing scheme that is defined in Section 5.7.8, “Configuring the DHCP Server As1 for Twinax Support” on page 157.

Note

It is not necessary to fully configure the DHCP server on the As1 system. Only the General and Address Pool options must be configured. No Options need to be provided.

Once the configuration is completed, ensure that the DHCP server is in a *stopped* state. The DHCP server does not need to be started. To be safe,

disable the subnet on the As1 system by right-clicking on the subnet and clicking on **Disable**.

Figure 81 shows the Operations Navigator display that shows the configured subnet. The current status of this subnet is *Disabled*.

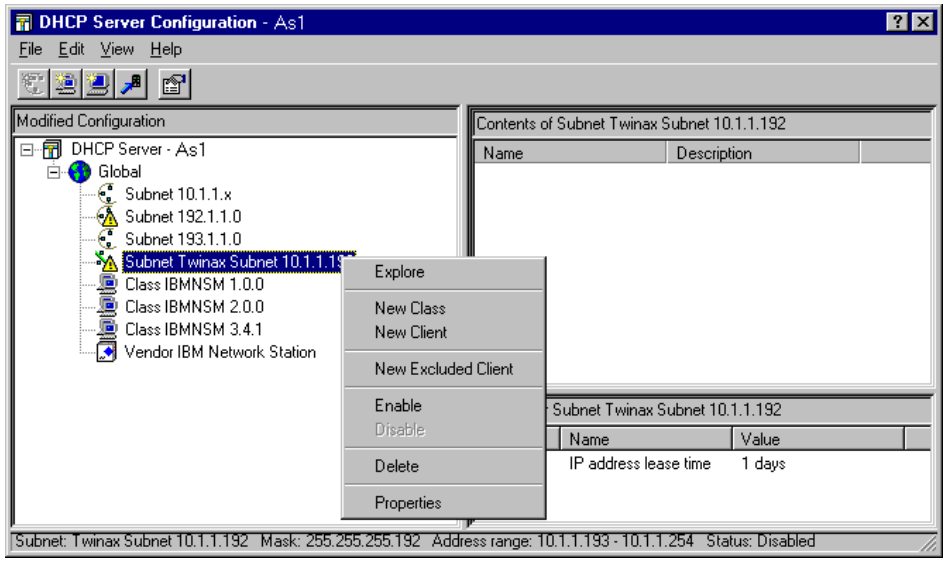


Figure 81. AS/400 Operations Navigator DHCP Configuration for Twinax Subnet on As1 System

Figure 82 on page 175 shows the TCP/IP servers display within Operations Navigator. From this figure, we see that the DHCP server on the As1 system is in a *stopped* state.

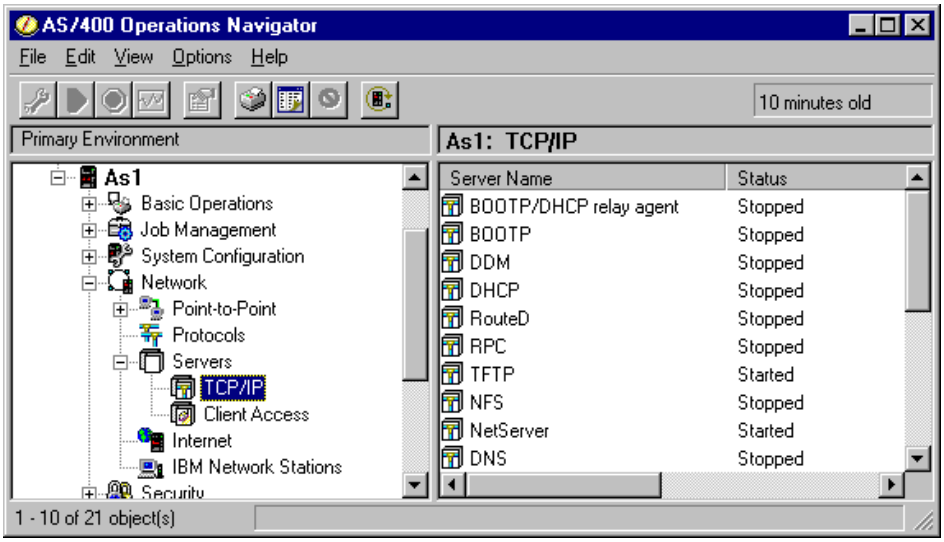


Figure 82. AS/400 Operations Navigator - TCP/IP Server Status

5.8.4 Power on the IBM Network Station

Start the twinax IBM Network Station to allow the AS/400 system to build the necessary TCP/IP interface and line description for the workstation controller. Power on the twinax attached IBM Network Station and look for the following messages:

- *NS0500 Search for Host System*
- *NS0930 Attempting to use DHCP*

These messages indicate that the AS/400 system has completed building the required TCP/IP interface for the workstation controller. Figure 83 on page 176 shows the resulting configuration display for the QTDL objects which were automatically created by the system.

```
                      Work with Configuration Status              AS1
                                                          09/21/98  12:10:15
Position to  . . . . .              Starting characters

Type options, press Enter.
  1=Vary on   2=Vary off   5=Work with job   8=Work with description
  9=Display mode status    13=Work with APPN status...

Opt  Description       Status               -------------Job--------------
     QTDL826400        ACTIVE
       QTDL8NET        ACTIVE
         QTDL8TCP      ACTIVE               QTCPIP      QTCP        006736
```

Figure 83. Automatically Created QTDL Descriptors

A TCP/IP interface has also been automatically created. You can view this by typing CFGTCP on a command line and then selecting option **1**. The resulting display is shown in Figure 84.

```
                        Work with TCP/IP Interfaces
                                                            System:   AS1
Type options, press Enter.
  1=Add   2=Change   4=Remove   5=Display   9=Start   10=End

     Internet         Subnet             Line      Line
Opt  Address          Mask            Description  Type
     10.1.1.2         255.255.255.0   TRLAN2       *TRLAN
     10.1.1.193       255.255.255.192 QTDL826400   *TDLC
     127.0.0.1        255.0.0.0       *LOOPBACK    *NONE
```

Figure 84. CFGTCP Option 1 Display Showing the TDLC Interface

Note

If only the message NS0500 is logged on the Network Station and there are no messages logged in QSYSOPR message queue, check the System Value QAUTOCFG. If this value is set to *OFF*, change it to **ON** before connecting and configuring twinax IBM Network Stations to your AS/400 system.

After the necessary configuration is created, you can power off the IBM Network Station and proceed to the next step.

5.8.5 Manually Changing the Auto Created TCP/IP Interface

For the twinax IBM Network Station to see and be seen across the network, the LAN interface of the As1 system must be manually added in the TCP/IP TDLC interface.

To add the LAN interface, complete the following steps:

1. From an AS/400 session, type `CFGTCP` on any command line.
2. Select option **1** (Work with interfaces).
3. To end the TDLC interface, select option **10**. In this scenario, the 10.1.1.193 interface is ended.
4. Select option **2** to change the interface.
5. Enter the value **10.1.1.2** on the *Associated local interface* parameter and press **Enter**. A display of the interface description is shown in Figure 85.
6. Start the TDLC interface.

```
                        Display TCP/IP Interface
                                                          System:   AS1
Internet address . . . . . . . . . . . . . . . :   10.1.1.193
Subnet mask  . . . . . . . . . . . . . . . . . :   255.255.255.192
Line description . . . . . . . . . . . . . . . :   QTDL826400
Line type  . . . . . . . . . . . . . . . . . . :   *TDLC
Associated local interface . . . . . . :   10.1.1.2
Interface status . . . . . . . . . . . . . . . :   Active
Type of service  . . . . . . . . . . . . . . . :   *NORMAL
Maximum transmission unit  . . . . . . . . . . :   *LIND
Automatic start  . . . . . . . . . . . . . . . :   *YES
```

Figure 85. TCP/IP Interface Updated with an Associated Local Interface Value

5.8.6 Configuring and Starting BOOTP/DHCP Relay Agent

After building the DHCP configuration file for the twinax subnet, it is time to turn *As1.mycompany.com* into a BOOTP/DHCP Relay Agent. In this scenario, the AS/400 BOOTP/DHCP Relay Agent is configured to forward DHCP messages directly, without delay, from the twinax subnet to the primary DHCP server.

To configure the AS/400 BOOTP/DHCP Relay Agent, complete the following steps:

1. Sign on to the AS/400 system As1.

2. From a command line, enter `CHGDHCPA MODE(*RELAY)`,and press **Enter**. This changes the mode of the DHCP server to be a BOOTP/DHCP Relay Agent.
3. From Operations Navigator, select **As1—>Network —>Servers —>TCP/IP** and right-click on **BOOTP/DHCP relay agent** as shown in Figure 86. Click on **Configuration** to select it.

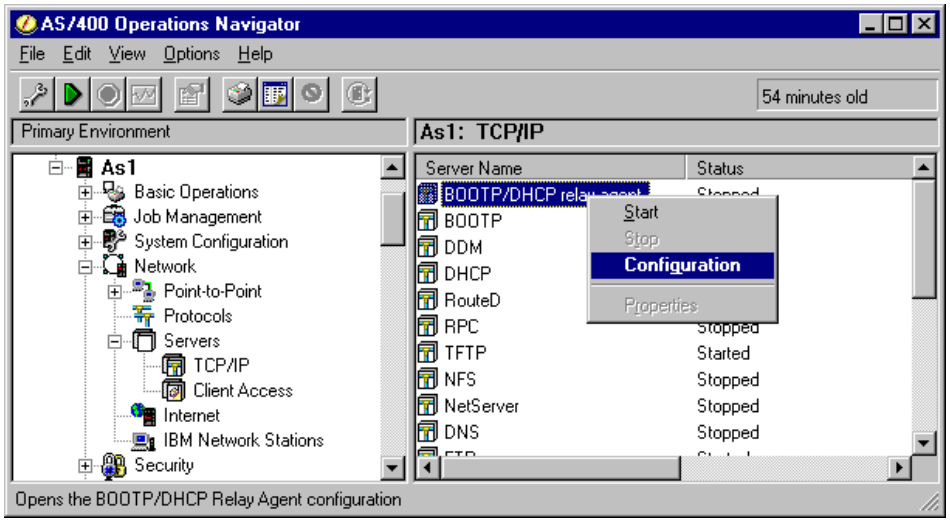


Figure 86. AS/400 Operations Navigator - Configuring BOOTP/DHCP Relay Agent

4. The BOOTP/DHCP Relay Agent properties window appears. Click the **Start when TCP/IP is started** check box to ensure that it is checked.
5. Click **Add**.
6. Use the pull-down option on the *Interface address* field to select the TCP/IP interface from which the BOOTP/DHCP Relay Agent accepts DHCP packets. This is the workstation controller interface was automatically created. Select the **10.1.1.193** interface.
7. Specify the IP address of the DHCP server to which the DHCP messages from the clients (IBM Network Stations) are sent. In this scenario the address that is used is **10.1.1.50**.

   Note: You can specify the system name in this option if your DNS server resolves IP addresses or if the host table on the system has been configured correctly.
8. Leave the *Maximum hops* set to the default of **4**.
9. Leave the *Packet transmission delay* at **0** (zero).

10.Click **OK**. The resulting display is shown in Figure 87.

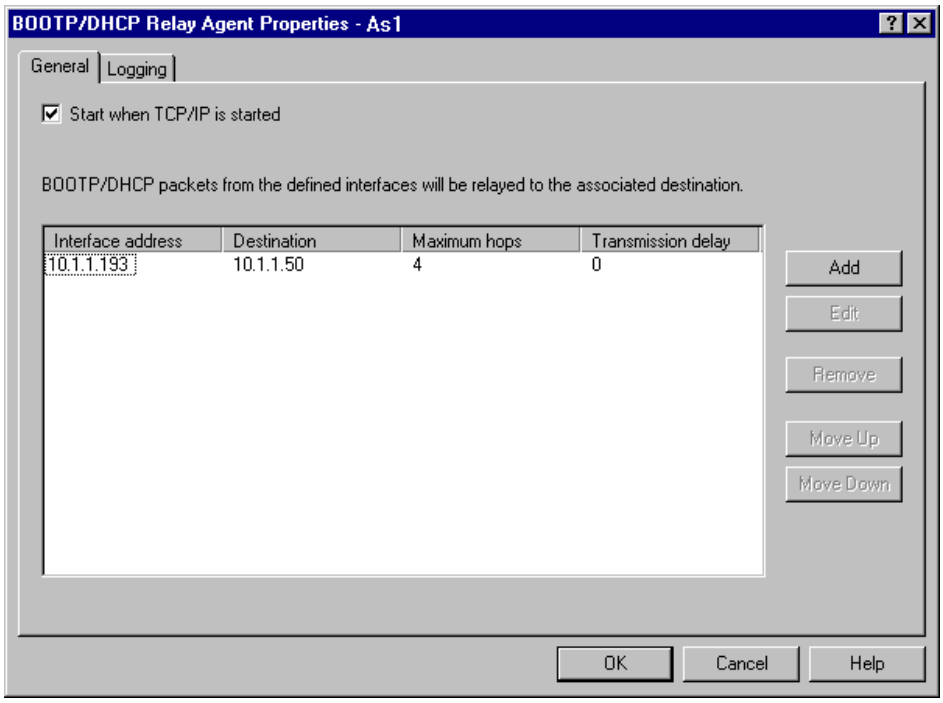


Figure 87. BOOTP/DHCP Relay Agent Configuration

11.From Operations Navigator, right-click **BOOTP/DHCP relay agent**. Select **Start** to start the server. The resulting status display is shown in Figure 88 on page 180.

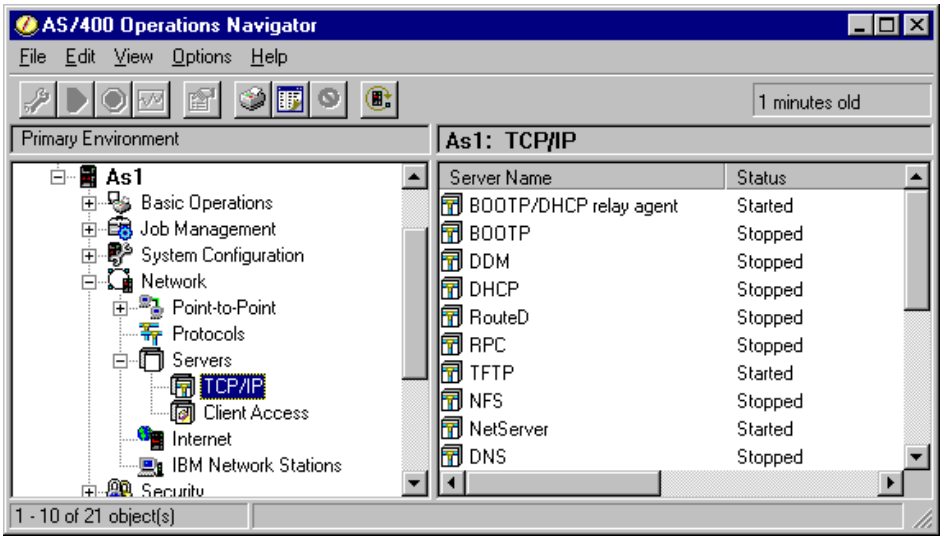


Figure 88. AS/400 Operations Navigator - TCP/IP Server Status

The BOOTP/DHCP Relay Agent now forwards DHCP messages from the workstation controller interface to the DHCP server, As2.

5.8.7 Changing the DHCP Server Configuration

The twinax subnet addresses that you use *must* be a subset of the address space 10.1.1.x. Because of this, the pool of addresses from 10.1.1.1 through 10.1.1.254 must be divided into two ranges. The pool must also be further reduced so that it does *not* include the addresses from 10.1.1.192 through 10.1.1.254, as these are used for the twinax subnet.

In this scenario, the address range from 10.1.1.1 through 10.1.1.254 is divided into two groups by applying masks to the range within the DHCP configuration. The two groups are then put back together, within the DHCP configuration, to form one group. DHCP option 1 is also used to specify the correct subnet mask to pass back to the client.

To divide the group into two ranges and allow the range to end at 10.1.1.192, a mask of 255.255.255.128 is applied in the DHCP configuration. This allows two groups of 128 addresses. The first group starts at 10.1.1.1 and ends at 10.1.1.127. The second group then has a mask of 255.255.255.192 applied to it. This creates a range of addresses from 10.1.1.128 through 10.1.1.191.

Refer to Figure 89 on page 181 for a visual representation of the address space from 10.1.1.1 through 10.1.1.191.

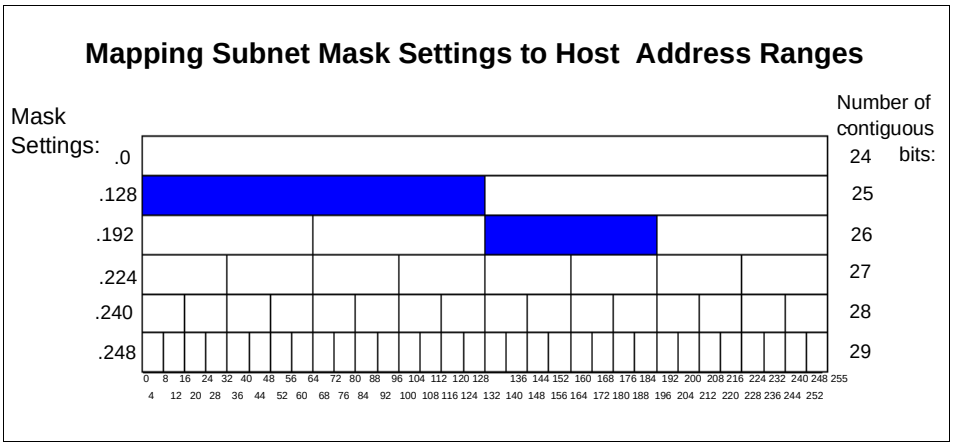


Figure 89. Applying Subnet Masks

These pools must be defined in the DHCP configuration. Complete these steps:

1. From Operations Navigator, select **As2 —>Network—>Servers —>TCP/IP.**
2. Right-click **DHCP**.
3. Ensure that **Global** is highlighted and right-click on it.
4. Select **New Subnet-Advanced** as shown in Figure 90 on page 182.

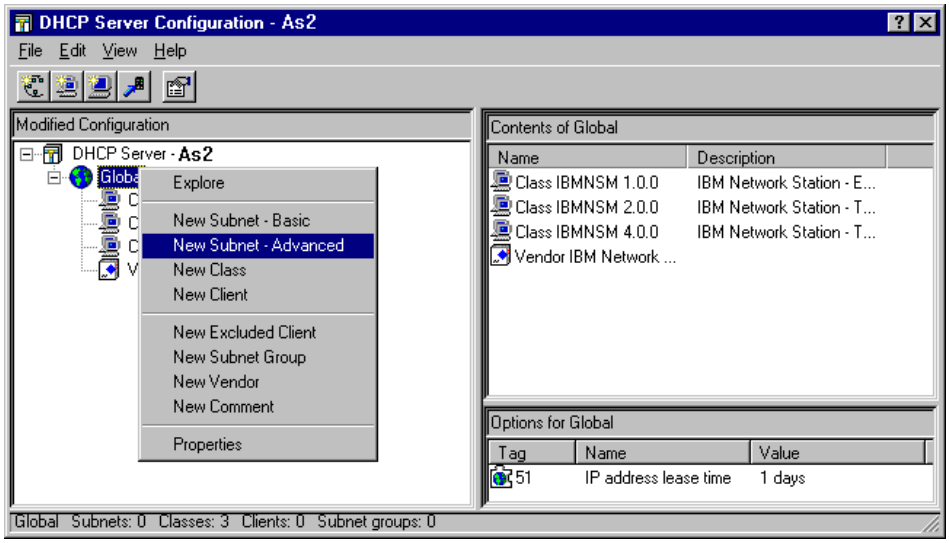


Figure 90. AS/400 Operations Navigator - Creating New Subnet in DHCP

5. Click on the **Address Pool** tab and fill in the Subnet address and the Subnet mask as shown in Figure 91 on page 183.
6. When you click on **Range to Assign**, the values are filled in automatically. Ensure that addresses 10.1.1.2 and 10.1.1.50 are excluded from the pool because these are the LAN IP interfaces for the AS/400 systems in this scenario.

The resulting Operations Navigator display for the first group is shown in Figure 91 on page 183.

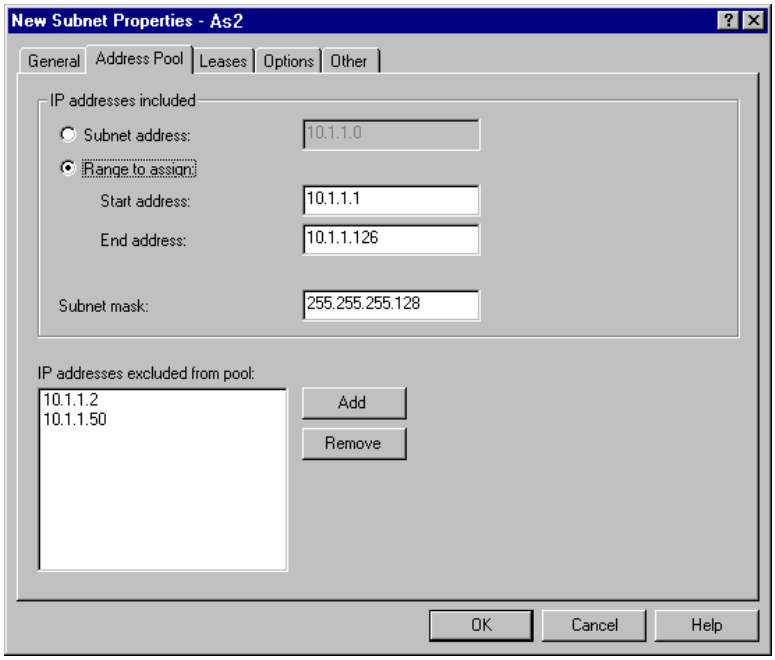


Figure 91. DHCP Configuration

The second group display is shown in Figure 92 on page 184.

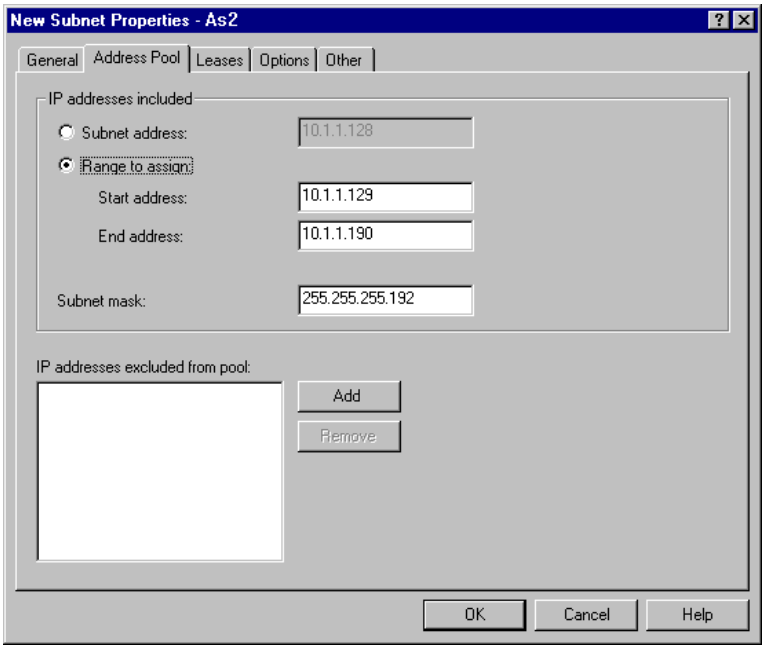


Figure 92. DHCP Configuration

Attention

For both of these groups, select the **Options** tab and configure DHCP option **1** to pass the real mask to use on this network, which is 255.255.255.0. You also must configure any other relevant options that clients on the main network require.

The next step is to group the two address ranges together again to form one pool in the DHCP server configuration.

To form a subnet group within the DHCP configuration, perform the following steps:

1. From the Operations Navigator DHCP, right-click **Global**.
2. Click **New Subnet Group** as shown in Figure 93 on page 185.

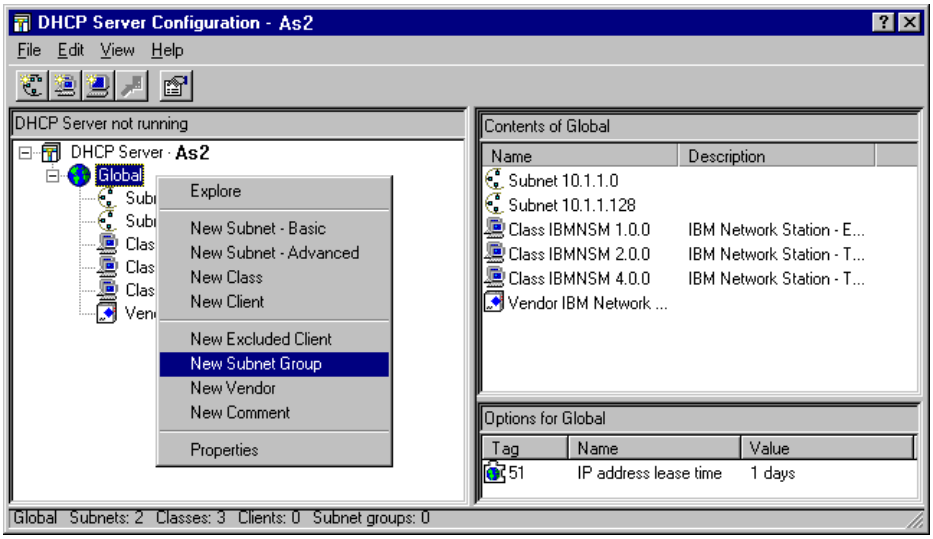


Figure 93. DHCP Configuration - Forming a New Subnet Group

3. Specify a valid description in the *Name* field. Blanks or special characters are not valid in this field. Refer to Figure 94 on page 186.

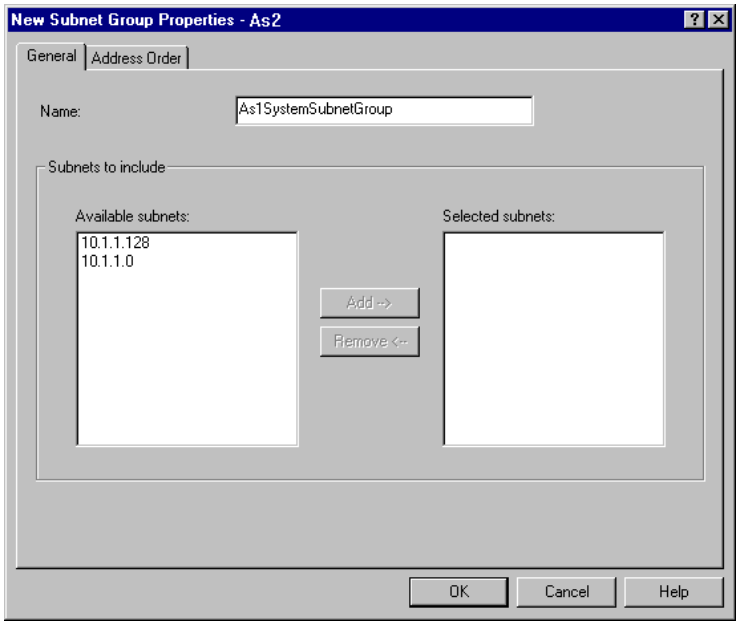


Figure 94. DHCP configuration - New Subnet Group Properties

4. Highlight the first address group, under the *Available subnets*, and click **Add**. Repeat this step for the second group. The resulting display is shown in Figure 95 on page 187.
5. Click the **Address Order** tab. Click either **In order** or **Balanced** to select the appropriate option. **In order** is the default.
6. Click **OK**. The resulting DHCP display is shown in Figure 96 on page 187.

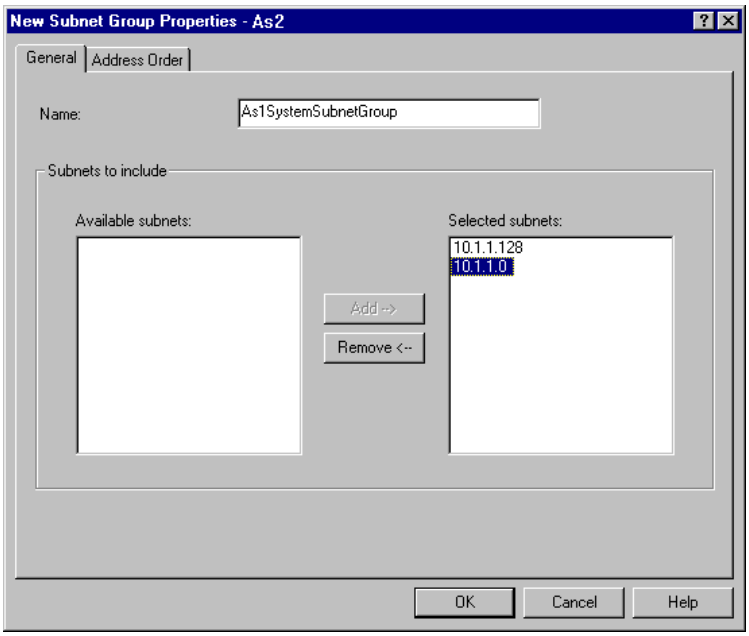


Figure 95. DHCP Configuration - Selection of Subnets for New Subnet Group

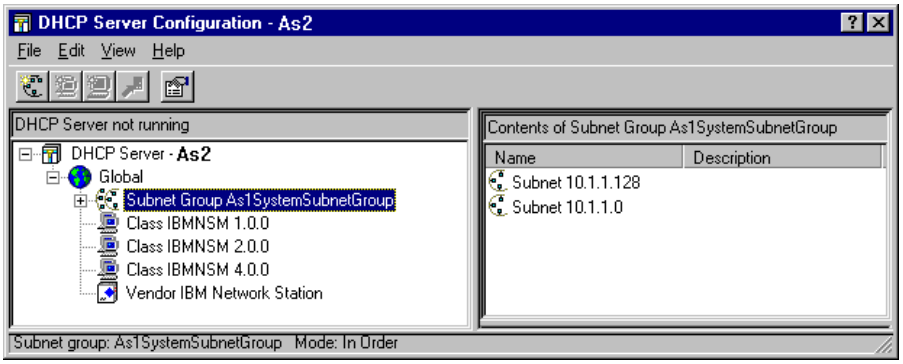


Figure 96. DHCP Configuration - Showing Contents of Subnet Group

5.8.8 Configuring the Twinax Subnet Address Pool

A TCP/IP address pool must be added on the primary DHCP server, As2. This provides network start-up information to the remote twinax client.

To accomplish this, a normal IP address pool must be configured because the twinax IBM Network Stations are not locally attached. A twinax subnet pool is

not configured as discussed in Section 5.7.8, “Configuring the DHCP Server As1 for Twinax Support” on page 157.

To configure the twinax subnet pool, complete the following steps:

1. Open the DHCP configuration, from Operations Navigator, on As2.
2. Right click **Global** and select **New Subnet - Advanced**.
3. Click **General** and enter the values as shown in Figure 97 on page 188.

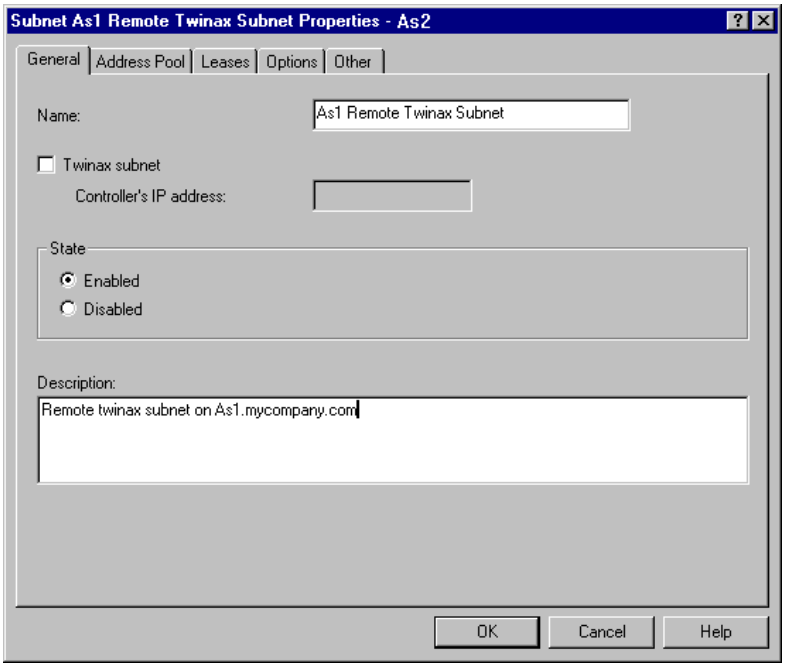


Figure 97. DHCP Configuration - New Subnet Group

Note: Ensure that the **Twinax subnet** box is left *unchecked*.

4. Click the **Address Pool** tab.
5. Click **Subnet Address** and specify the twinax subnet address as **10.1.1.192**.
6. Enter the mask **255.255.255.192** into the *Subnet mask* field.
7. Click **Range to assign**. The addresses are automatically filled in. See Figure 98 on page 189 for the resulting display.

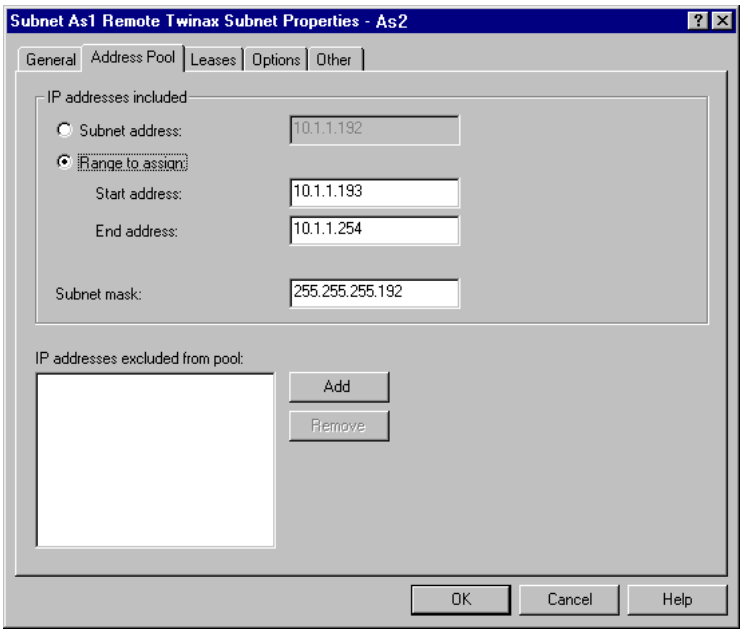


Figure 98. DHCP Configuration - Remote Twinax IP Address Pool

8. Click the **Options** tab and add the options shown in Table 19.

Table 19. Options and Values

Option	Value
1 Subnet Mask	255.255.255.192
3 Router	10.1.1.193 (the WSC is the first hop for the devices)
66 Server name	10.1.1.193
67 Boot file name	/QIBM/ProdData/NetworkStation/kernel

9. Click **OK**. The resulting display is shown in Figure 99 on page 190.

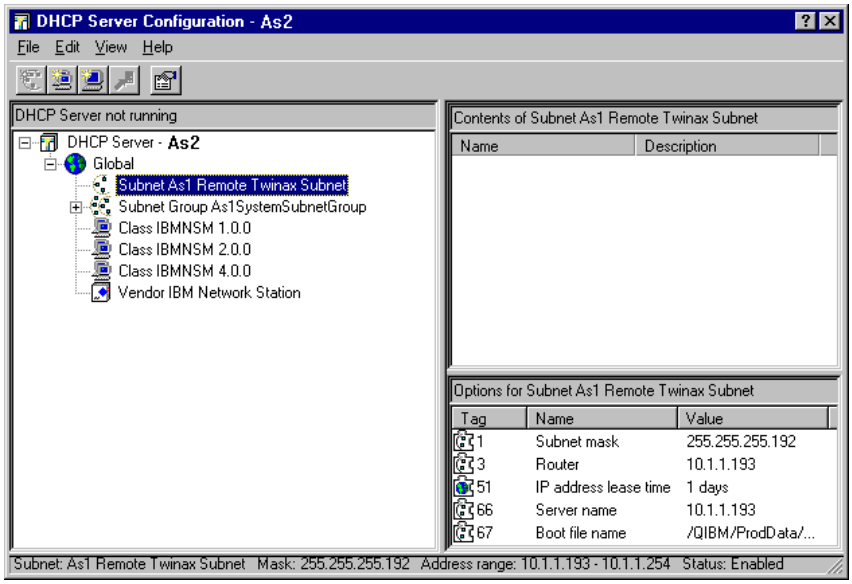

DHCP Server Configuration - As2
File Edit View Help
DHCP Server not running
DHCP Server - As2
Global
Subnet As1 Remote Twinax Subnet
Subnet Group As1SystemSubnetGroup
Class IBMNSM 1.0.0
Class IBMNSM 2.0.0
Class IBMNSM 4.0.0
Vendor IBM Network Station
Contents of Subnet As1 Remote Twinax Subnet
Name
Description
Options for Subnet As1 Remote Twinax Subnet
Tag
Name
Value
1 Subnet mask 255.255.255.192
3 Router 10.1.1.193
51 IP address lease time 1 days
66 Server name 10.1.1.193
67 Boot file name /QIBM/ProdData/...
Subnet: As1 Remote Twinax Subnet Mask: 255.255.255.192 Address range: 10.1.1.193 - 10.1.1.254 Status: Enabled

Figure 99. Operations Navigator - DHCP Configuration Display Showing Subnet Groups

10.Update or start the DHCP server on the *As2* system.

5.8.9 Starting the IBM Network Station

When the DHCP configuration has completed correctly, the twinax IBM Network Station can be powered on. The Network Station should now boot to completion.

5.8.10 Testing Connectivity

In this scenario a 5250 TELNET session was started to both the *As1.mycompany.com* and *As2.mycompany.com* systems. Both attempts were successful.

5.8.11 Summary

This scenario included building a DHCP configuration file on the local AS/400 system, As1, from which the workstation controller receives the necessary network information.

The first IBM Network Station that powers on causes the workstation controller to query the DHCP configuration file. The AS/400 system automatically builds the necessary TDLC configuration and an associated

TCP/IP interface. It was then necessary to manually change the TCP/IP interface to include the As1 LAN address as the Associated Local Interface.

The As1 system was then configured as a BOOTP/DHCP Relay Agent. This relay agent was configured and started through Operations Navigator. The configuration was set to forward DHCP messages from the locally attached twinax subnet to the remote DHCP server, As2.

The address pool, 10.1.1.x, was split within the DHCP configuration on the As2 system. The two configured pools were then re-grouped to form a single pool within DHCP.

An IP address pool for the remote twinax subnet was configured, within DHCP, on the As2 system. The DHCP server was then started on the As2 system.

After the configuration was complete the IBM Network Station was again started. However, this time the DHCP messages were forwarded by the local DHCP/BOOTP Relay Agent (As1) to the remote DHCP server, As2. The IBM Network Station then obtained the necessary network start up information that it required to boot up successfully.

5.9 Twinax IBM Network Station with Remote Boot Server

It is possible to have the IBM Network Station send a request to a DHCP server, for network information, and have that information returned. The returned information contains the name or IP address of another host that serves the IBM Network Station with its kernel and user configuration.

You can also configure the AS/400 DHCP server to provide the options that are necessary to instruct the IBM Network Station to load its kernel from a server other than the DHCP server host. Up to two systems can be specified from which the user configuration data can be loaded.

Figure 100 on page 192 shows a twinax Network Station attached to an AS/400 system, As1. In this scenario, the twinax Network Station goes to As1 system for its network configuration. The As1 system then replies to the Network Station that it should go to address 10.1.1.50, system As2, for the kernel and configuration data. The Network Station then accesses As2, using the workstation controller and the LAN for its base code and configuration data.

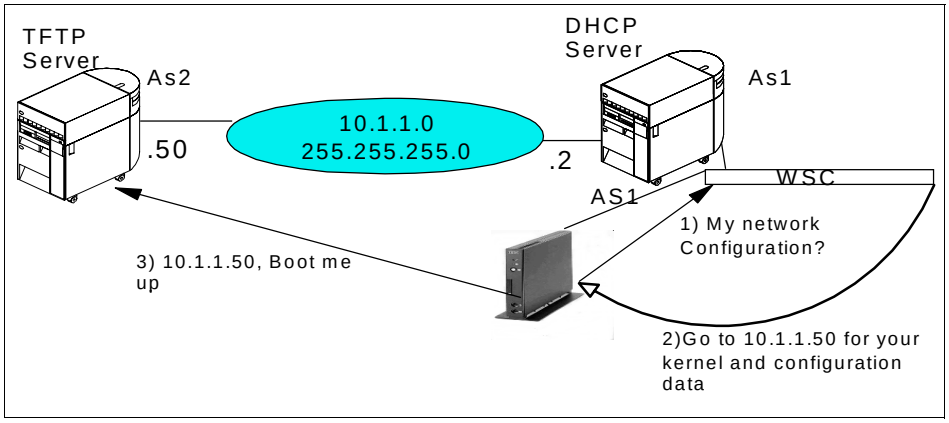


Figure 100. Twinax Attached Network Station Obtaining Network Configuration

5.9.1 Scenario Overview

This scenario shows an example of a twinaxial Network Station attached to a local workstation controller on an AS/400 system. This AS/400 system is a DHCP server and provides the network configuration to the Network Station. It also provides the address of the base code server and the terminal configuration server to the Network Station. In this scenario, the As2 system is the system that the As1 system directs the Network Station to for its base code and terminal configuration server.

The As2 system is set up with the TFTP server running and the Network Station Login Daemon server.

5.9.2 Scenario Objectives

The objectives of this scenario are to:

- Configure twinax-attached IBM Network Stations.
- Configure the DHCP server, As1, to provide the locally attached twinax IBM Network Stations with network configuration.
- Configure the DHCP server, As1, to provide information to the attached twinax IBM Network Stations on where to -obtain kernel and configuration data.
- Start the Network Station and ensure LAN connectivity.

5.9.3 Scenario Advantages

The advantages of this scenario include:

- Easier to connect twinax-attached IBM Network Stations to an existing network
- Multiple servers do not need to exist on one system but can be configured on different systems
- Routing of datagrams, from the twinax subnet to the attached LAN and vice versa, occurs automatically

5.9.4 Scenario Disadvantages

There is a requirement for an extensive understanding of DHCP. The variety of options required to setup within the DHCP configuration is the main disadvantage.

5.9.5 Scenario Network Configuration

Figure 101 shows the network topology used for this scenario. The twinax attached Network Stations are connected to the DHCP server, As1. The IBM Network Stations receive their start-up information from the As1 system and then are directed to the As2 system for their base and configuration code.

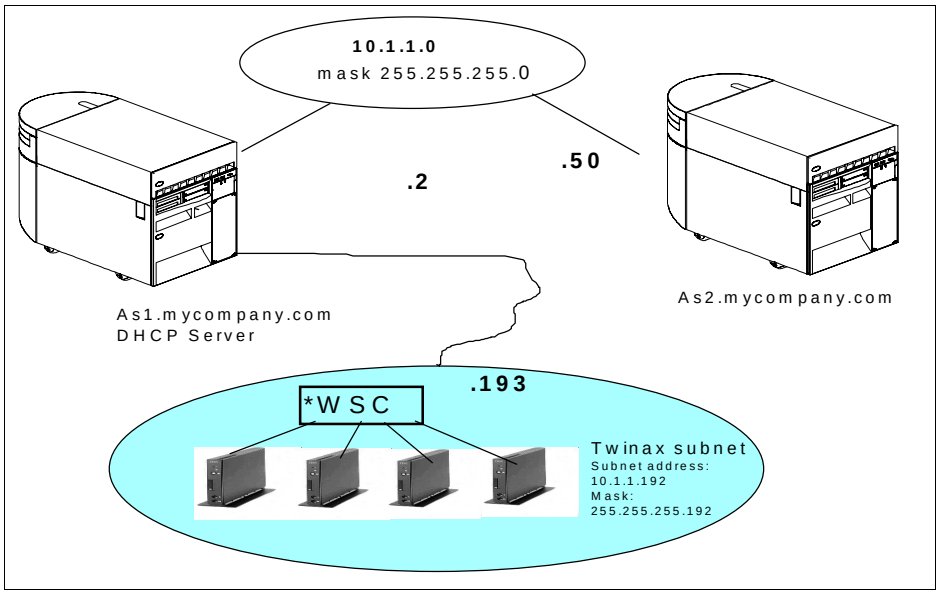


Figure 101. Network Topology for Remote Boot Server Scenario

5.9.6 Task Summary

Note

It is assumed, in this scenario, that the DHCP server on the As1 system already functions correctly and supports the attached twinax Network Stations. If this is not the case, refer to Section 5.7, “Twinax IBM Network Station with Local DHCP Server Scenario” on page 154. This section outlines the necessary steps needed to configure the DHCP server for twinax support.

The following tasks are required to complete this scenario:

1. Configure the DHCP server As1 for returning information to the twinax subnet that contains the IP address of a base and configuration server.
2. Ensure that the proper TCP/IP servers are started on the As2 system.
3. Configure and start the twinax IBM Network Station.
4. Test connectivity.

5.9.7 Configuring the DHCP Server on As1

Note

The Operations Navigator displays, shown in this section, were captured from a PC running IBM AS/400 Client Access for Windows 95/NT Version 3 Release 2 Modification Level 0.

We will configure a boot server for the IBM Network Station. This is different from the DHCP server to which the Network Station is connected.

To configure the boot server, complete the following steps:

1. Use the AS/400 Operations Navigator on System As1 to open the DHCP server configuration window. Right click on the Twinax Subnet that was previously configured. Highlight **Properties**. The resulting display is shown in Figure 102 on page 195.

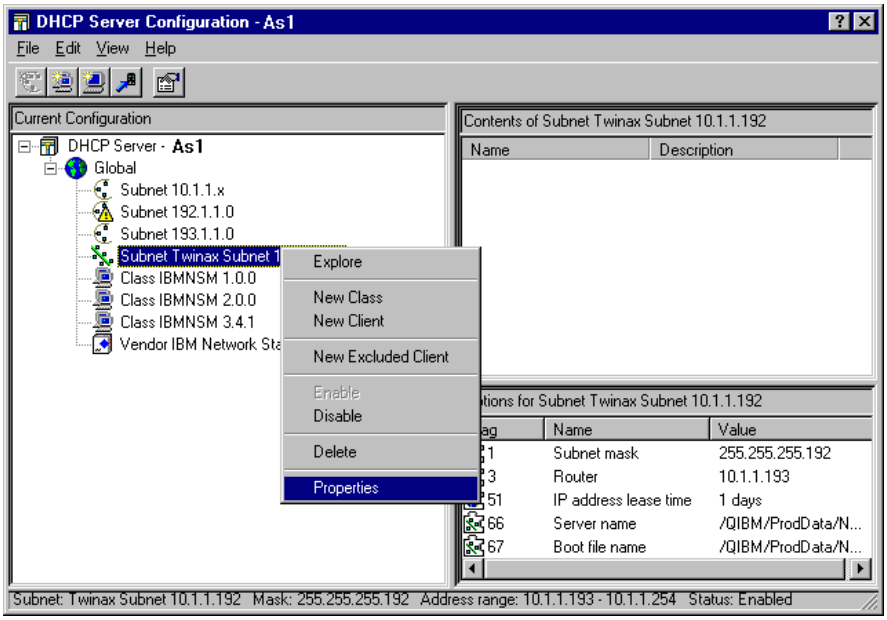


Figure 102. Operations Navigator - DHCP Twinax Subnet Properties

2. Click the **Options** tab.
3. From the previous DHCP configuration, options **1**, **3**, **66** and **67** were defined. They are shown in the *Selected options*. For this scenario, however, option **66** must be modified to show the address of the TFTP server: 10.1.1.50. See Figure 103 on page 196 for the resulting display.

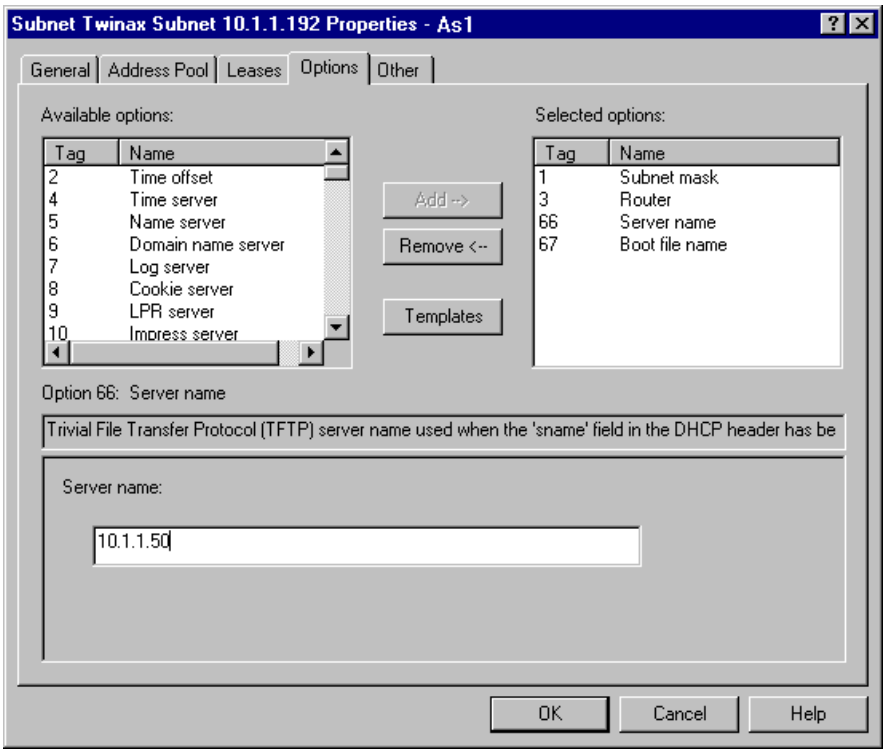


Figure 103. DHCP Configuration - Defining TFTP Server

4. Click **Templates**.
5. Click **New**. To add user option **211** (protocol to use for loading the user configuration data), specify the data as shown in Figure 104 on page 197.

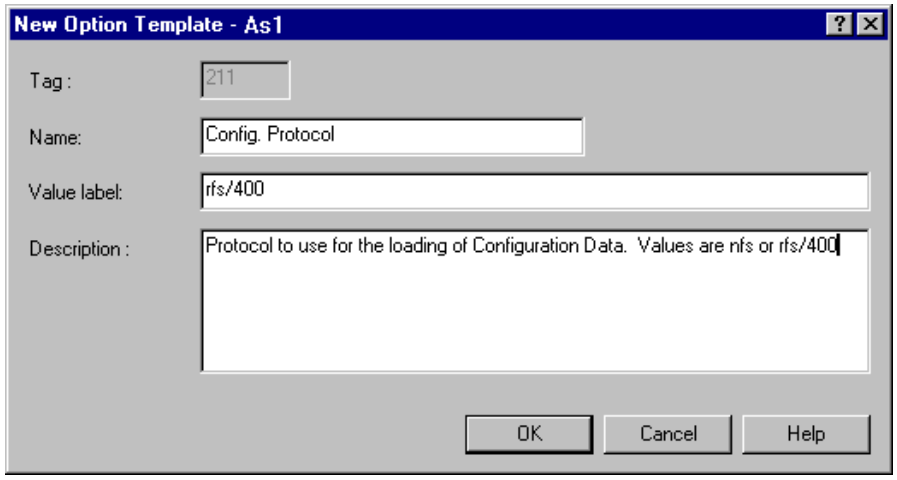


Figure 104. DHCP Configuration - Option 211 Configuration Protocol Template

6. Click **OK**.
7. Repeat the steps 4 and 5 to add the user options **212**, **213** and **214** as shown in Figure 105, Figure 106 on page 198, and Figure 107 on page 198.

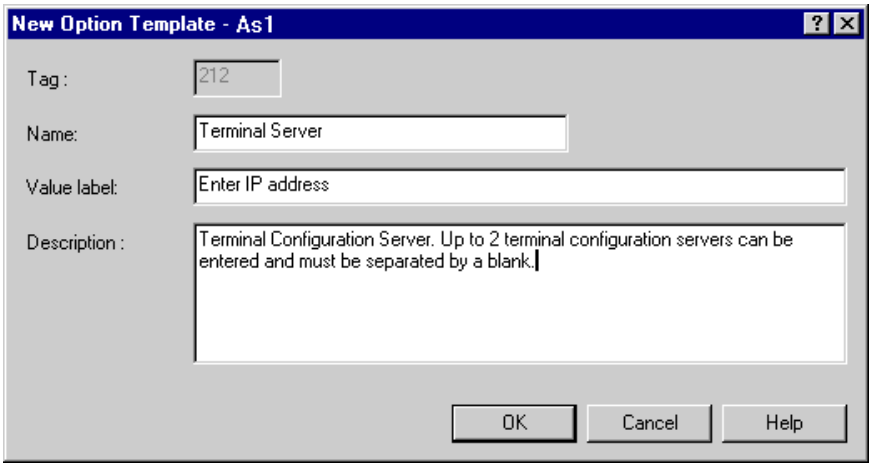


Figure 105. DHCP Configuration - Option 212 Terminal Server Template

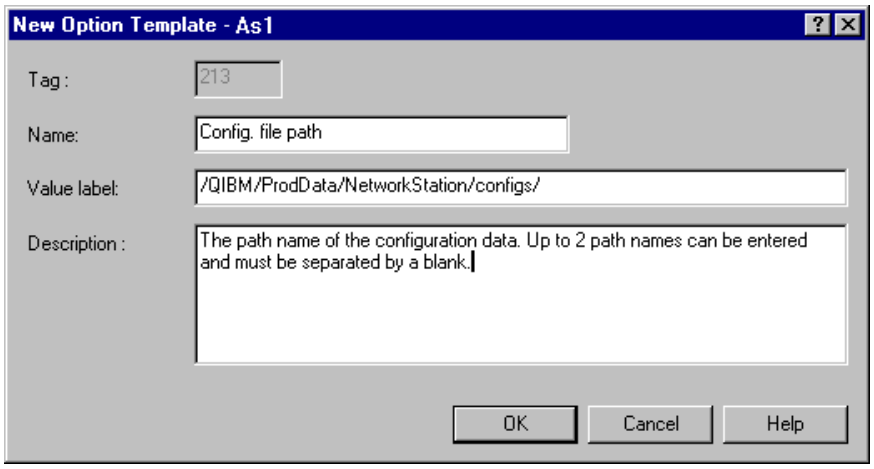


Figure 106. DHCP Configuration - Option 213 Configuration File Path Template

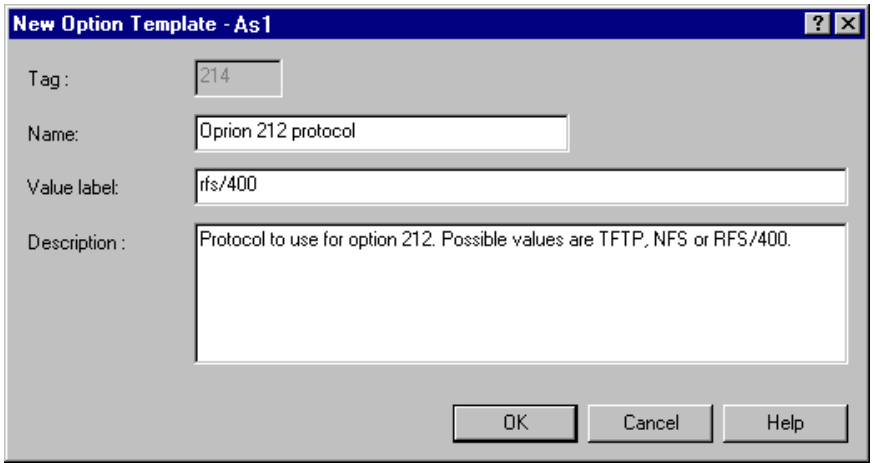


Figure 107. DHCP Configuration - Option 214 Protocol to Use Template

8. You are returned to the main *Options* display. Under the *Available options* scroll down to the end of the list to see that options 211 through 214 have been added. The resulting display is shown in Figure 108 on page 199.

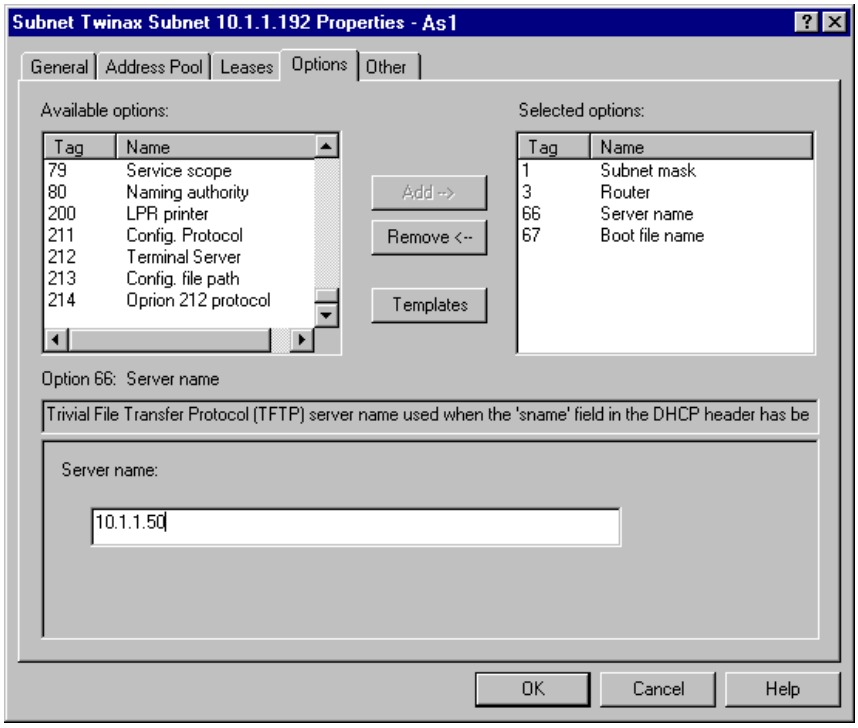


Figure 108. DHCP Configuration - Viewing Available Options

9. The newly defined tags must now have the corresponding values added. For each of the tags from 211 to 214, click the TAG number in the Available options window and then click **Add** to add the value into the *Selected options*. Figure 109 on page 200, Figure 110 on page 201 through Figure 112 on page 203 shows the addition of these tags.

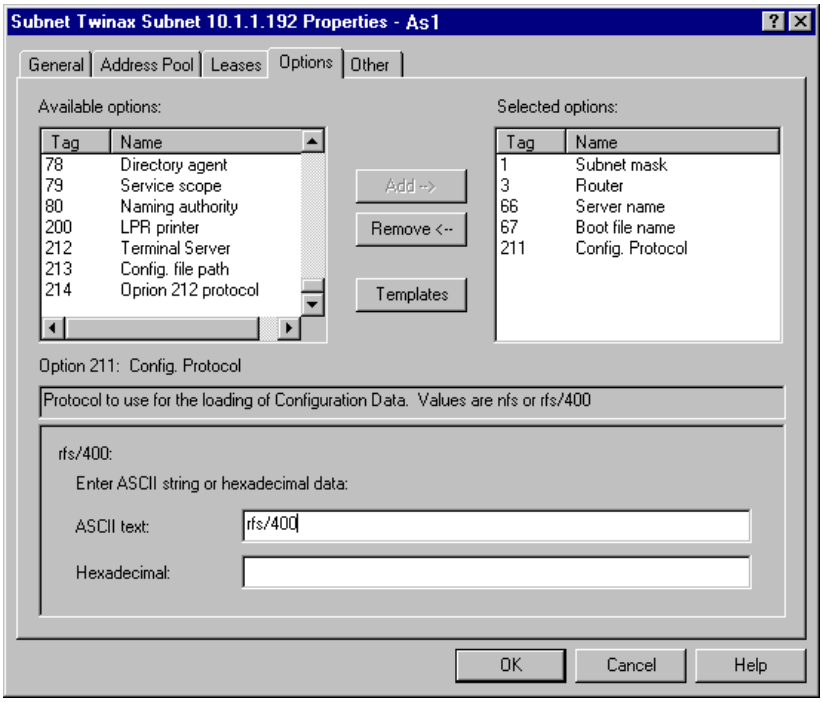


Figure 109. DHCP Configuration - Adding Tag 211 Configuration Protocol

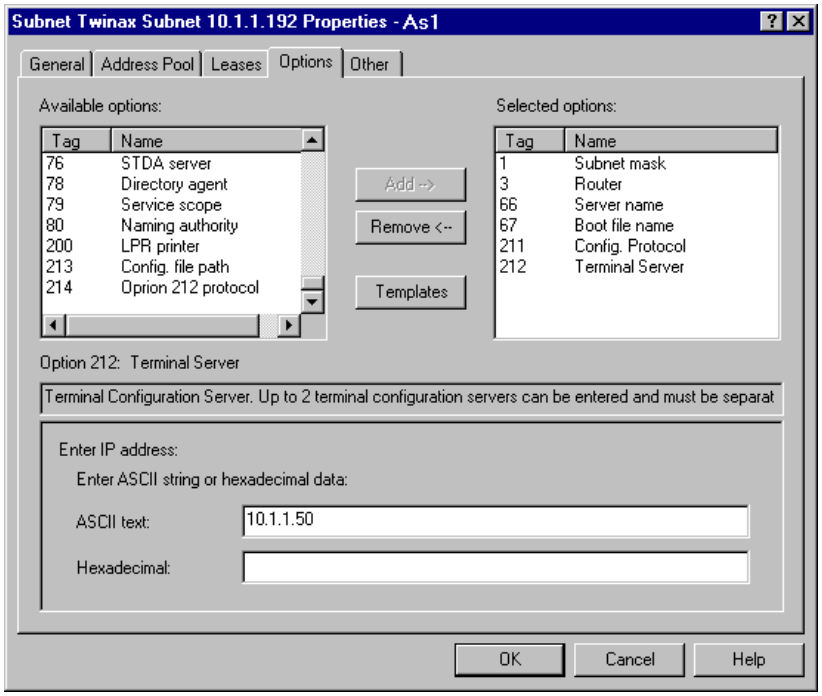


Figure 110. DHCP Configuration - Adding Tag 212 Terminal Server

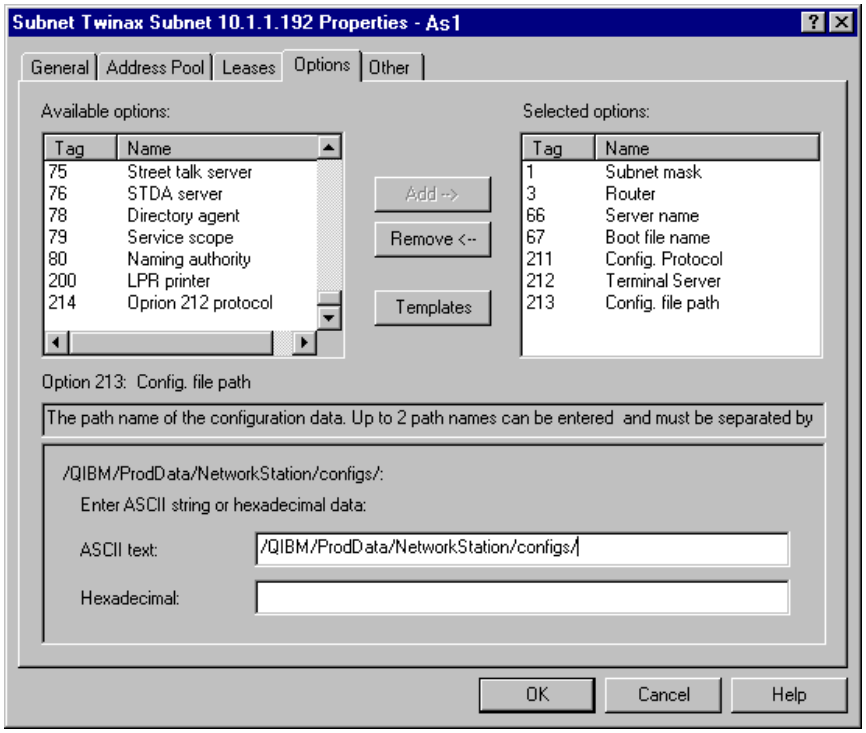


Figure 111. DHCP Configuration - Adding Tag 213 Configuration File Path

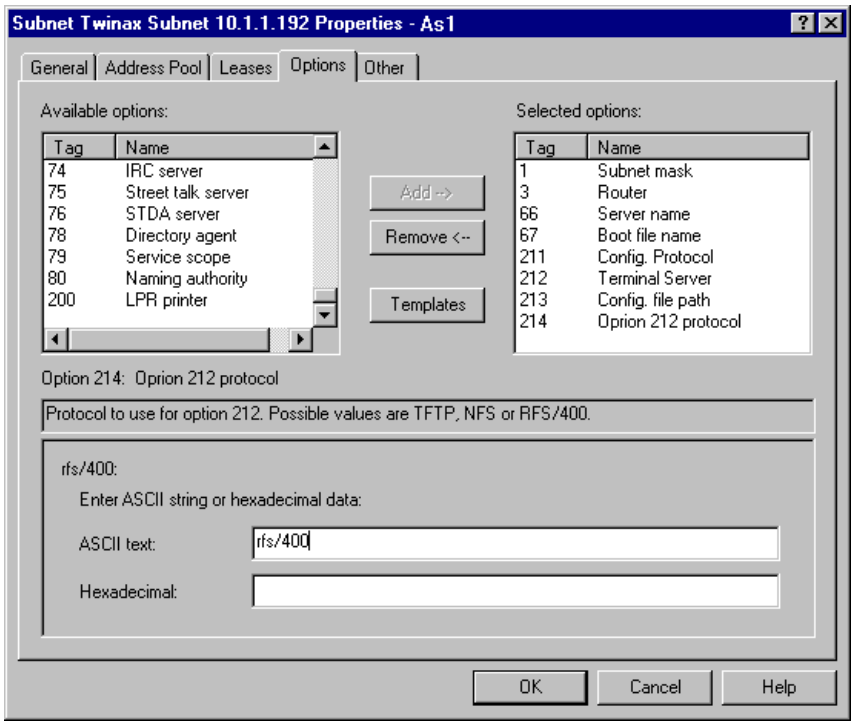


Figure 112. DHCP Configuration - Adding Tag 214 Protocol

10. After the tags are added, click **OK**. You are returned to the main DHCP server display. With the twinax subnet still highlighted, the options are shown with their corresponding Hexadecimal data. The resulting display is shown in Figure 113 on page 204.

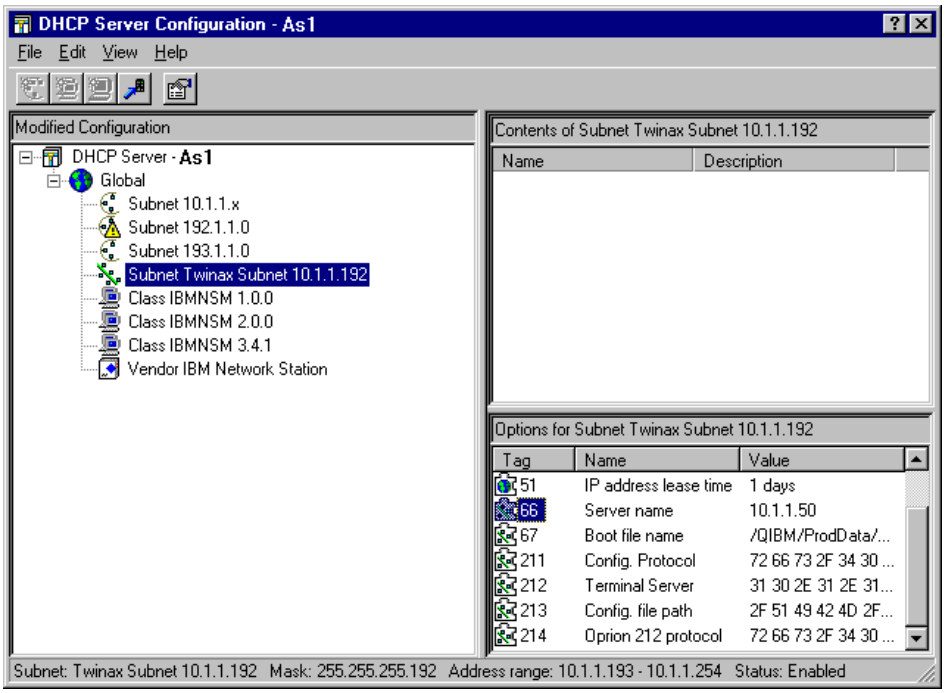

DHCP Server Configuration - As1
File Edit View Help
Modified Configuration
DHCP Server - As1
Global
Subnet 10.1.1.x
Subnet 192.1.1.0
Subnet 193.1.1.0
Subnet Twinax Subnet 10.1.1.192
Class IBMNSM 1.0.0
Class IBMNSM 2.0.0
Class IBMNSM 3.4.1
Vendor IBM Network Station
Contents of Subnet Twinax Subnet 10.1.1.192
Name
Description
Options for Subnet Twinax Subnet 10.1.1.192
Tag
Name
Value
51 IP address lease time 1 days
66 Server name 10.1.1.50
67 Boot file name /QIBM/ProdData/...
211 Config. Protocol 72 66 73 2F 34 30 ...
212 Terminal Server 31 30 2E 31 2E 31...
213 Config. file path 2F 51 49 42 4D 2F...
214 Oprion 212 protocol 72 66 73 2F 34 30 ...
Subnet: Twinax Subnet 10.1.1.192 Mask: 255.255.255.192 Address range: 10.1.1.193 - 10.1.1.254 Status: Enabled

Figure 113. Operations Navigator - Modified DHCP Configuration Display

11. Close the DHCP window. You are prompted to update the server. Click **Yes** on this window. If the server is already running, stop and restart the server from Operations Navigator.

5.9.8 Ensuring the Proper TCP/IP Servers are Started on As2

The TFTP Server and the Network Station Login Daemon Server must both be started on the As2 system for this scenario. This can be checked through a *green screen* interface entering the command, `NETSTAT *CNN`. The resulting display is shown in Figure 114 on page 205. Notice that the Network Station Login Daemon uses port 256.

The status of these servers can also be checked using Operations Navigator. The resulting display is shown in Figure 115 on page 205.

```
                    Work with TCP/IP Connection Status
                                                          System:   As2
Local internet address  . . . . . . . . . . . :   *ALL

Type options, press Enter.
  4=End   5=Display details

     Remote          Remote     Local
Opt  Address         Port       Port       Idle Time  State
     *               *          ftp-con >  014:37:50  Listen
     *               *          telnet     000:00:05  Listen
     *               *          smtp       183:47:21  Listen
     *               *          tftp       013:53:47  *UDP
     *               *          www-http   018:21:35  Listen
     *               *          pop3       183:47:11  Listen
     *               *          snmp       141:49:43  *UDP
     *               *          256        013:49:59  Listen
     *               *          as-svrmap  000:00:22  Listen
```

*Figure 114. Netstat *CNN Display Showing Active TCP/IP Servers*

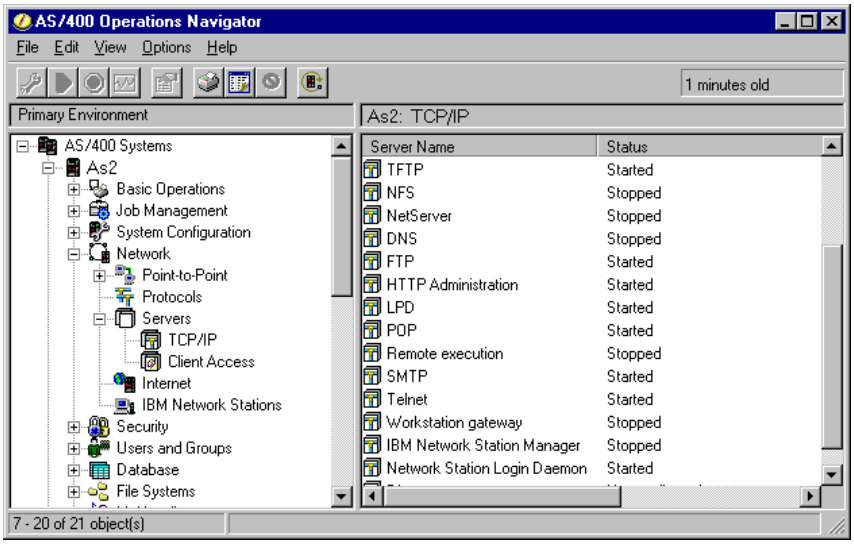


Figure 115. Operations Navigator - TCP/IP Server Status Display

5.9.9 Configuring and Starting the Twinax IBM Network Station

As mentioned prevously, it is assumed that the DHCP server on As1 fully supports the attached twinax Network Stations. There exists a QTDL line, controller, device and an TCP/IP interface for this same QTLD line. The TCP/IP interface has an *Associated local interface* that points to the LAN

adapter of the system. In this case, this parameter has the value of 10.1.1.2. A display device also exists for each of the attached Network Stations.

Note

If your system currently does not have DHCP configured and running, refer to Section 5.7, “Twinax IBM Network Station with Local DHCP Server Scenario” on page 154 for instructions on how to set up the DHCP server.

Figure 116 and Figure 117 show the information that can be viewed within the Network Station’s Setup Utility. However, these displays are what you see *before* the Network Stations are powered up in this scenario. The Setup Utility can be accessed by powering off the Network Station and then powering it back on. When the message, NS0500 *Search for Host System* ,is shown on the display, press **ECS**.

```
                        IBM Network Station
                     Set Network Parameters

IP Addressed from ............................. NVRAM

Boot Host IP Address:
  First Host ..................................... 10.1.1.193
  Second Host .................................... 0.0.0.0
  Third Host ..................................... 0.0.0.0

Configuration Host IP Address:
  First Host ..................................... 0.0.0.0.
  Second Host .................................... 0.0.0.0
```

Figure 116. Set Network Parameters Display (Before Bootup)

Note

Figure 117 on page 207 shows the *NVRAM* settings. However, when the Network Station is ready to boot, the F3 display must show the *Network* setting.

```
                    IBM Network Station
                Set Configuration Parameters

Configuration File .........................

Configuration Directory:
  First ..................................... /QIBM/ProdData/NetworkStation/con
                                              figs/
  Second .....................................

Configuration Host Protocol:
  First ..................................... Default
  Second .................................... Default
```

Figure 117. Set Configuration Parameters Display (Before Bootup)

The Network Station is now ready to be powered up. The messages seen on the initial display, when the Network Station is powering up, are similar to what is shown in Figure 118.

```
NS0500  Search for Host System ...
NS0930  Attempting to use DHCP ...... successful
NS1090  System 10.1.1.50 contacted from 10.1.1.194
NS0520  Request startup information ...
NS0530  Loading startup information ...
```

Figure 118. Sample Messages on Network Station during Startup

The NS1090 message shows that the Network Station has contacted the As2 system, which has an IP address of 10.1.1.50.

When the bootup is completed, a login display is shown from the 10.1.1.50 system, As2.

If the Setup Utility is now reviewed, on the Network Station, the display shows updated information as shown in Figure 119 on page 208 and Figure 120 on page 208.

```
                        IBM Network Station
                      Set Network Parameters

IP Addressed from ............................... NVRAM

Boot Host IP Address:
  First Host ..................................... 10.1.1.193
  Second Host .................................... 0.0.0.0
  Third Host ..................................... 0.0.0.0

Configuration Host IP Address:
  First Host ..................................... 10.1.1.50
  Second Host .................................... 0.0.0.0
```

Figure 119. Set Network Parameters Display (After Bootup)

```
                      IBM Network Station
                   Set Configuration Parameters

Configuration File .........................

Configuration Directory:
  First ..................................... /QIBM/ProdData/NetworkStation/con
                                              figs/
  Second .....................................

Configuration Host Protocol:
  First ..................................... RFS/400
  Second .................................... Default
```

Figure 120. Set Configuration Parameters Display (After Bootup)

5.9.10 Testing Connectivity

After the Network Station is powered up and is signed on, TELNET 5250 sessions can be started to both the As1 and As2 systems.

5.9.11 Summary

This scenario showed the DHCP configuration on an AS/400 system that supported attached twinax IBM Network Stations. The DHCP configuration involved modifying the twinax subnet so that the twinax Network Stations obtain their kernel and configuration data from another server, As2.

No change was required on the Network Station itself. However, it required a power off and a power on after the required DHCP configuration was completed on system As1.

Chapter 6. Problem Determination

This section outlines some of the more commonly used tools that can help you in diagnosing some common IBM Network Station errors.

6.1 Viewing the IBM Network Station Console Log

The IBM Network Station maintains a system log of almost every event that has occurred on the Network Station. This system log can be very useful in helping to diagnose configuration problems with your Network Station.

There are two methods to view the system log of the IBM Network Station. You can use TELNET to gain access to the Network Station on port 5998 or you can access the system log locally from the IBM Network Station.

Tip

To enhance the messages logged to the system console log, you can turn on an extended diagnostics message by placing the following line in the *defaults.dft* file and restart the Network Station:

```
set file-extended-diagnostics = true
```

6.1.1 Accessing the System Log Using TELNET

Complete the following steps to use TELNET to view a system log for an IBM Network Station from a Windows 95 platform:

1. From the Windows 95 task bar, select **Start**, then select **Run**.
2. Type **TELNET** into the dialog box and press **Enter**.

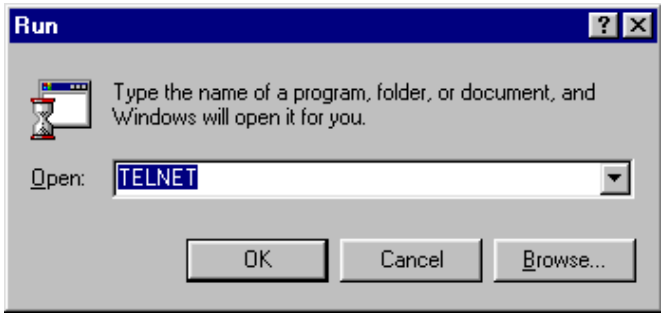


Figure 121. Windows 95 RUN Dialog Box

© Copyright IBM Corp. 1999

3. From the file pulldown menu select **Terminal.**
4. Select **Preferences**
5. Change the *Buffer size* to **9999**, as shown in to Figure 122. This enables you to scroll back through the entire console log file.

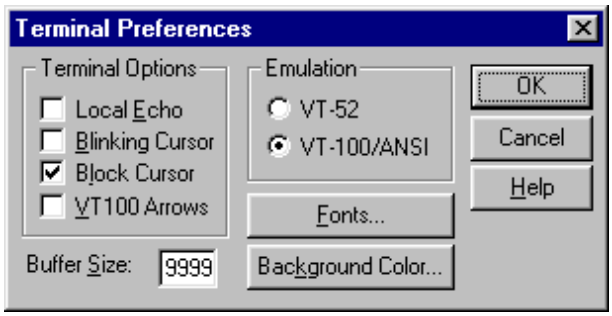


Figure 122. TELNET Terminal Preferences

6. Click on **OK**.
7. Select **Connect** from the file pull down menu.
8. Click on **Remote System**.
9. Enter the TCP/IP address of the desired Network Station and the console log port ID of **5998**. Please refer to Figure 123.

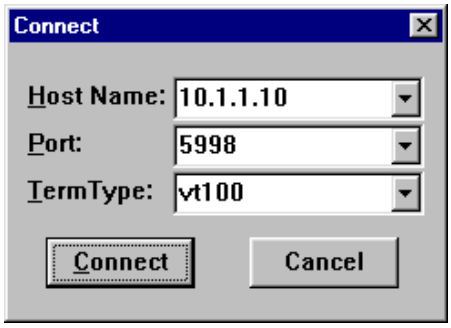


Figure 123. TELNET Terminal Connection Dialog Box

10. Click on **Connect**.
11. The console scrolls by as it fills up the buffer space within the Telnet Terminal session. The vertical scroll bar enables you to scroll back through the log file.

6.1.2 Accessing the System Log Using the Console Manager

You can also view the system log directly on the Network Station by accessing the User Services Console.

The following steps assume you were able to start the Network Station and have the Login display on the display, or you have signed on and authenticated against a host server.

Use the follow steps to view the console log (see Figure 124):

1. Press **Alt + Shift + Home** to start the Network Station User Service console.
2. Click on **Messages** to view the log.
3. Use the vertical scroll bar to move up and down through the log file.

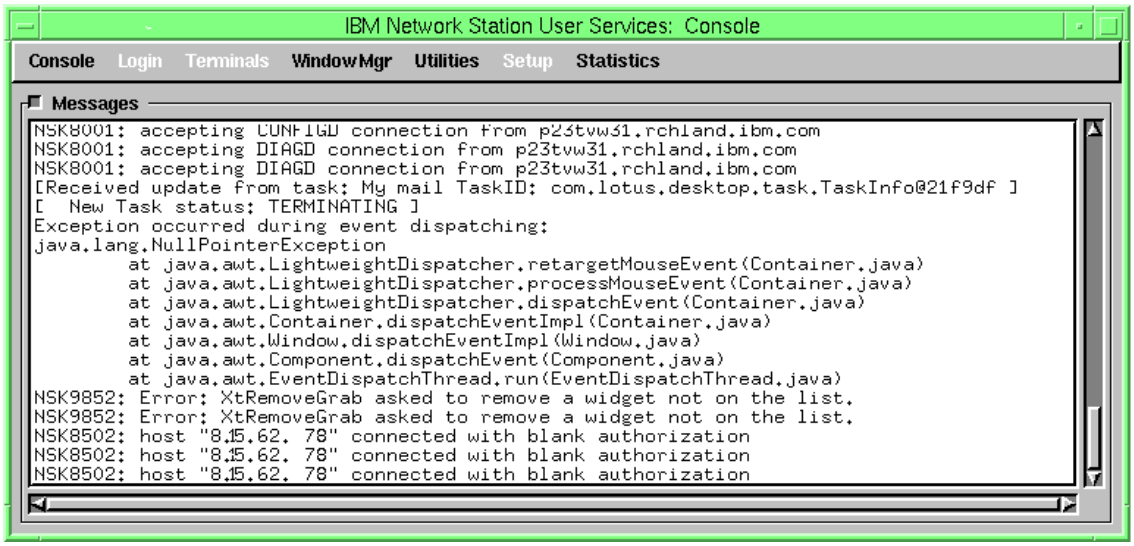

IBM Network Station User Services: Console
Console
Login
Terminals
WindowMgr
Utilities
Setup
Statistics
Messages
NSK8001: accepting CONFIGD connection from p23tvw31.rchland.ibm.com
NSK8001: accepting DIAGD connection from p23tvw31.rchland.ibm.com
NSK8001: accepting DIAGD connection from p23tvw31.rchland.ibm.com
[Received update from task: My mail TaskID: com.lotus.desktop.task.TaskInfo@21f9df]
[New Task status: TERMINATING]
Exception occurred during event dispatching:
java.lang.NullPointerException
at java.awt.LightweightDispatcher.retargetMouseEvent(Container.java)
at java.awt.LightweightDispatcher.processMouseEvent(Container.java)
at java.awt.LightweightDispatcher.dispatchEvent(Container.java)
at java.awt.Container.dispatchEventImpl(Container.java)
at java.awt.Window.dispatchEventImpl(Window.java)
at java.awt.Component.dispatchEvent(Component.java)
at java.awt.EventDispatchThread.run(EventDispatchThread.java)
NSK9852: Error: XtRemoveGrab asked to remove a widget not on the list.
NSK9852: Error: XtRemoveGrab asked to remove a widget not on the list.
NSK8502: host "8.15.62. 78" connected with blank authorization
NSK8502: host "8.15.62. 78" connected with blank authorization
NSK8502: host "8.15.62. 78" connected with blank authorization

Figure 124. Console Log Example

Chapter 7. Replicating a Remote Boot Server Environment

If you determine that remote boot servers are the best option for your planned remote IBM Network Station users, one of your next tasks is to develop an implementation plan. In addition, you must make a key decision about whether you will use the separation of servers function or if your remote boot servers will also act as authentication servers.

Another task in your plan is determining how (and when) the IBM Network Station Manager product is installed on your remote servers. The normal, supported installation method, found in the manual , can used to install the 5648-C05 CDs or you can download the code from the Web. However, this chapter discusses an alternative method for getting the IBM Network Station Manager for AS/400 product installed on the remote servers. Your implementation plan should also include a task that determines if there are common or unique system-wide, group or user level desktop preferences for the remote site users. Additional information on planning for TCP/IP and IBM Network Stations is included in the manual *IBM Network Station Manager Installation and Use,* SC41-0664.

The following sections discuss several example scenarios for replicating the IBM Network Station Manager environment from a central boot server to remote boot servers. Please notice that these methods have not been tested by development and therefore are not formally supported

7.1 Centralized Authentication Server

In this scenario, assume that a central AS/400 (AS1) system located at company headquarters in New York is connected to twenty remote AS/400 systems through an existing TCP/IP based wide area network. The central AS/400 system, at V4R3 and Release 3 of IBM Network Station Manager for AS/400, was installed for a recently completed pilot. Because the IBM Network Station pilot was successful, the decision was made to begin a roll out of IBM Network Stations at each of the twenty remote sites. Because these remote AS/400s are at V4R3, they are capable of running IBM Network Station Manager for AS/400 Release 3. The *planned* network diagram is shown in Figure 125 on page 214. The first remote site is in St. Louis. The AS2 AS/400 system installed there has V4R3 installed with a number of PCs currently connected to it on an Ethernet LAN. The plan is to replace a number of existing under-utilized, out-dated PCs with IBM Network Stations and leave the more current PCs in place for those users who need a PC.

© Copyright IBM Corp. 1999

In developing the implementation plan, the company decided to use the central AS/400 system at headquarters to authenticate the IBM Network Station users at the remote sites. In this case, the Release 3 IBM Network Station Manager for AS/400 is used for the separation of servers function. The AS1 AS/400 system in New York acts as a base code server for the IBM Network Stations in New York and also provide the DHCP, Authentication and Terminal Configuration server functions to all IBM Network Stations. The AS2 AS/400 system in St. Louis acts as a base code server for the IBM Network Stations located in that remote site.

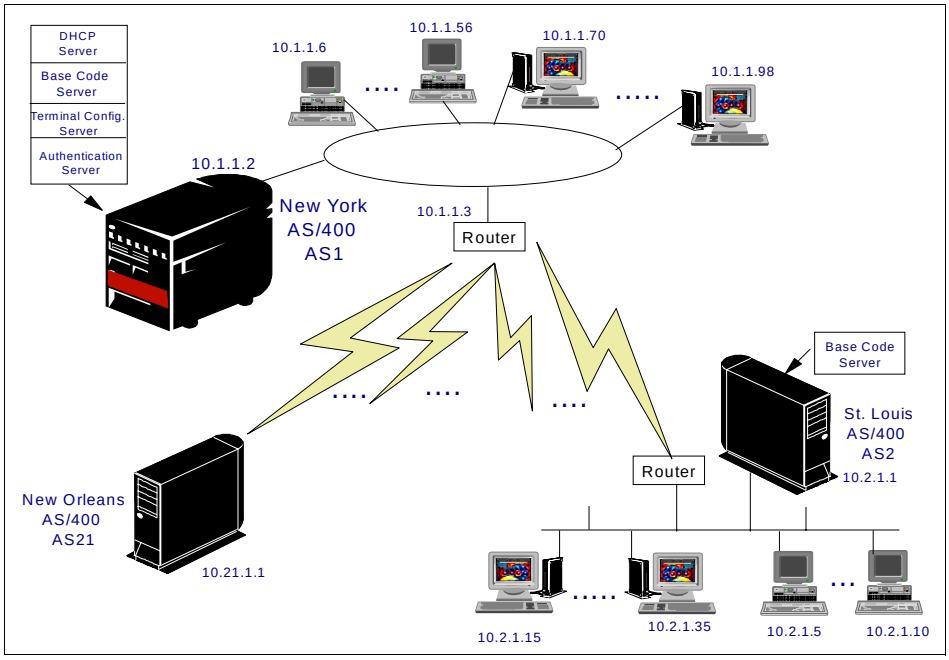


Figure 125. Replicating Remote Boot Servers - Centralized Authentication Server

7.1.1 IBM Network Station Manager Replication to Remote Server

Because the central site AS/400 system is providing the authentication server function for all IBM Network Stations, the objective in this scenario is to easily *copy* the IBM Network Station Manager for AS/400 product from the installed central site to the remote AS2 AS/400 server which allows it to act as a base code server. In this environment, the users in St. Louis have user IDs on both AS/400 systems because they need to access applications running on both the headquarters AS/400 system, AS1 and their *local* AS/400 system, AS2.

Because our central and remote system are both at the same OS/400 V4R3 level, the document referenced at the end of this paragraph was used to verify that there were no prerequisite PTFs required before installing IBM Network Station Manager for AS/400 on AS2. However, if the remote server had been at an earlier release level, we would need to verify that the prerequisite PTFs were installed before doing the following steps. In addition, the steps involving saving products and files change would need to reflect the correct target release. The prerequisite PTFs for each OS/400 version/release/modification level are listed on the Web site: as400service.ibm.com in the AS/400 Software Knowledge Database. The title of the document is *OS/400 Pre-Req PTFs for 5648C05 (NSM R3)*.

Use the following steps to replicate the IBM Network Station Manager for AS/400 environment to the remote server:

1. On the central AS1 AS/400 (source system), use the following command to create a save file to contain the IBM Network Station Manager for AS/400 product and its installed PTFs.

   ```
   CRTSAVF FILE(WORKLIB/C05SAVF) TEXT('savf for savlicpgm of 5648C05')
   ```

2. On the central AS1 AS/400, use the following command to *save* the IBM Network Station Manager for AS/400 product to the previously created save file.

   ```
   SAVLICPGM LICPGM(5648C05) DEV(*SAVF) SAVF(WORKLIB/C05SAVF)
   TGTRLS(*CURRENT)
   ```

3. From the central AS1 system, use the following commands to FTP the *C05SAVF* containing the 5648-C05 product to the remote server:

   ```
   ftp as2
   (Enter user ID and password as prompted.)
   bin
   cd /QSYS.LIB/as2work.lib/
   lcd worklib
   put c05savf
   ```

4. On the target system AS2 (for example, the remote server), use the following command:

   ```
   RSTLICPGM LICPGM(5648C05) DEV(*SAVF) OPTION(*BASE) RSTOBJ(*ALL)
   SAVF(AS2WORK/C05SAVF)
   ```

   Messages similar to the following should appear near the bottom of your joblog, indicating a successful installation.

   ```
   Object moved.
   Object moved.
   Object moved.
   ```

```
Object moved.
Object moved.
Object QAYTCSNC1P in QUSRSYS type *FILE created.
1 objects duplicated.
Ownership of object QAYTCSNC1P in QUSRSYS type *FILE changed.
Object STRNSSA in QSYS type *CMD deleted.
Object STRNSSA in QSYS type *CMD created.
1 objects duplicated.
Ownership of object STRNSSA in QSYS type *CMD changed.
Object QAYTCSNC1 in QUSRSYS type *FILE created.
1 objects duplicated.
Ownership of object QAYTCSNC1 in QUSRSYS type *FILE changed.
File QAYTCSNC1P started journaling to journal QYTCSJRN.
Migration program completed successfully.
*LNG objects for NLV 2924 for product 5648C05 option *BASE release
*FIRST restored.
Objects for product 5648C05 option *BASE release *FIRST restored.
```

5. On the remote server, run the Start Network Station Setup Assistant (STRNSSA) command to start the Network Station setup assistant. Go through *each* task and sub-task as appropriate, even though the *Completed* column may already indicate a status of YES.

   Note: If you receive a message in your job log indicating that *...task 5000 failed/port 80 was not active*, start the HTTP server default instance by running the command, `STRTCPSVR SERVER(*HTTP) HTTPSVR(DEFAULT)`, and then re-try task 5000)

6. Because the *c*entral AS/400 server (10.1.1.2*)* is used to authenticate the IBM Network Station users in St. Louis, the *defaults.dft* configuration file on AS2 in St. Louis must be modified. In this example, FTP was used to download this file from the */QIBM/UserData/NetworkStation/StationConfig* IFS directory to a PC. Wordpad was used to insert the following statements into the *defaults.dft* file.

   Note: 10.1.1.2 in the -authserv statement is the IP address of the Authentication server.

   ```
   set exec-startup-commands = {
   { mcuis }
   { "actlogin -authserv 10.1.1.2" }
   }
   ```

7. Use FTP to upload the modified *defaults.dft* file to the AS2 AS/400 remote server. You can also rename this file to *remdef.dft* and FTP it up to the central AS1 AS/400 server. You can FTP the file numerous times as *defaults.dft* to the various remote AS/400 base code servers.

8. In this case, since DHCP is being used, ensure that the DHCP server options are set up correctly on AS1 server so that the IBM Network Stations in St. Louis have AS2 server as their base code server. For example, option 66 would point to different TFTP servers to allow IBM Network Stations in different locations to get their base code from the appropriate server. For more details on DHCP configuration, refer to the manual, *IBM Network Station Manager Installation and Use,* SC41-0664 and *TCP/IP Configuration and Reference*, SC41-5420, available online at www.ibm.com/nc/pubs, and www.as400service.ibm.com respectively. In addition, the *AS/400 TCP/IP Autoconfiguration: DNS and DHCP*, SG24-5147 is available online at: www.redbooks.ibm.com

Refer to the manual *IBM Network Station Manager Installation and Use,* SC41-0664, for performance tuning information. It is available online at the Web site: www.ibm.com/nc/pubs

After completing the steps, the IBM Network Stations at the remote site were powered on or re-booted. They were able to obtain their base code from their local AS2 AS/400 server and authenticate against the central AS1 AS/400 server.

7.2 Decentralized Authentication Server

In this example, the central site in Chicago has an AS/400 system (SYSAS1), a S/390 system (SYS390), and a development AS/400 system (SYSAS3) installed. In addition, sixty remote AS/400 systems are installed across a TCP/IP based wide area network. The central AS/400 system (SYSAS1) in Chicago has V4R3 and Release 3 of IBM Network Station Manager for AS/400 already installed because they recently completed an IBM Network Station pilot project. Because the IBM Network Station pilot was successful. An implementation of IBM Network Stations at the various remote sites was also planned. The planned network is shown in Figure 126 on page 218. Although, the normal installation process using either the shipped 5648-C05 CDs or the downloaded code from the Internet and group PTF SF99082 can be used (as documented in the manual *IBM Network Station Manager Installation and Use,* SC41-0664), the company decided that a replication technique would be used instead. We choose the development AS/400 system (SYSAS3) to be the *master remote server copy* for replicating the *master* IBM Network Station Manager environment to the remote servers.

Because the remote sites are primarily autonomous and do not want to rely on the connection to the central site to obtain user preferences, decentralized authentication was selected. However, for ease of installation, the decision

was made to *copy* the base IBM Network Station Manager environment to the remote sites from the AS/400 system, SYSAS3 at the central site. In addition, common system-wide and group-level preferences were determined. Because they applied to all remote servers, the changes were made on the master SYSAS3 system before replication. IBM Network Station Manager on SYSAS3 was used to omit the 3270 button from the system default desktop for the remote sites because the majority of remote users do not need access to the S/390 system in Chicago. There is a set of users at each remote site that do need S/390 access. Therefore, a group profile called *grp3270* was created. The desktop preferences for the *grp3270* group was changed so that a 3270 button appears on those users' IBM Network Station menu bars.

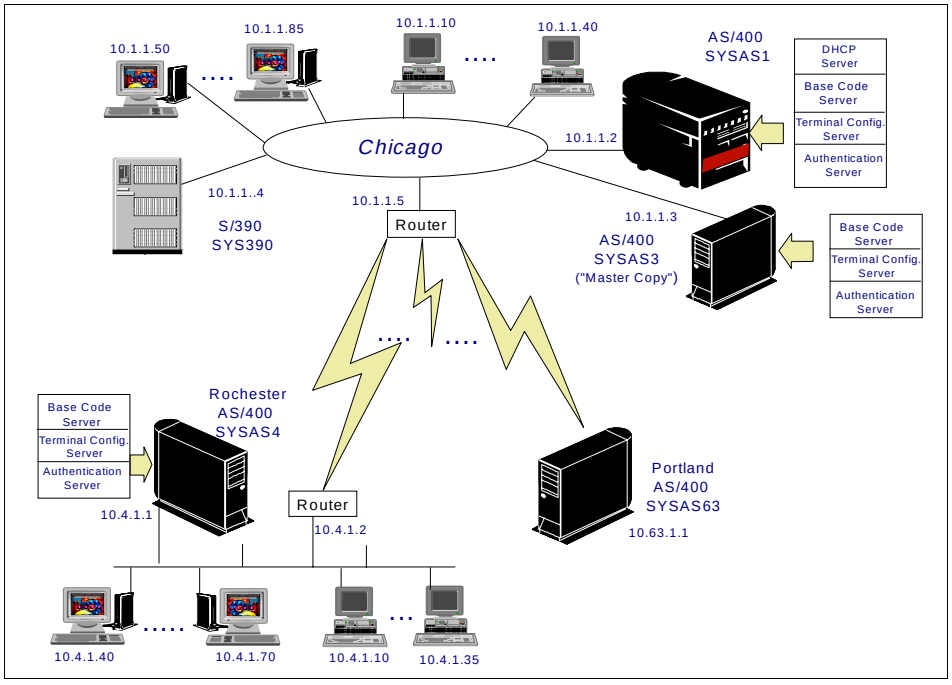


Figure 126. Replicating Remote Boot Servers - Decentralized Authentication

7.2.1 IBM Network Station Manager Replication to Remote Server

The plan is to use the Network Station Manager environment on the central site development AS/400 (SYSAS3) system as a *master copy* and replicate it to the remote AS/400 boot servers. The AS/400 system, SYSAS1, continues to be a production boot server for the IBM Network Station users located at the central site. Our central and remote system are both at the same OS/400 V4R3 level. We used the document referenced at the end of this paragraph to

verify that there were no prerequisite PTFs required prior to installing IBM Network Station Manager for AS/400 Release 3. However, if the remote server had been at an earlier release level, then we would need to ensure that the prerequisite PTFs were installed before doing the following steps. The prerequisite PTFs are listed for each OS/400 version/release/modification level in the AS/400 Software Knowledge Database on the Web site: as400service.ibm.com

The title of the document is *OS/400 Pre-Req PTFs for 5648C05 (NSM R3)*.

Note

The following steps were used in an environment where both the source and the target systems were at OS/400 V4R3. These steps were *not* tested with systems at different OS/400 levels. As a result, the following steps could change if systems at different levels are used. For example, you would possibly need to change the target release on the *save* commands and install prerequisite PTFs on target AS/400 systems having a release prior to V4R3 installed (or one different from the source system).

After determining which (if any) system wide, group or user preferences were common to all remote servers and therefore, be set on the source (SYSAS3) system, the following steps were used to set up and then replicate the *master remote* IBM Network Station Manager environment from SYSAS3 system to the remote AS/400 server, SYSAS4.

1. As shown in Figure 127 on page 220, use IBM Network Station Manager to omit the 3270 button from the System Defaults Menu Setup Task by removing the check mark for *Include default menu bar buttons (5250, 3270 and NC Navigator)* and then, adding a 5250 Session button again. Complete the process by adding an NC Navigator button as shown in Figure 128 on page 220.

Tip

${BOOTHOST} can be used in the AS/400 system parameter if a session to the boot server is desired. In this case, rather than the user being prompted for an AS/400 system name or IP address, a 5250 session to the associated remote boot server is started when the 5250 menu bar button is selected.

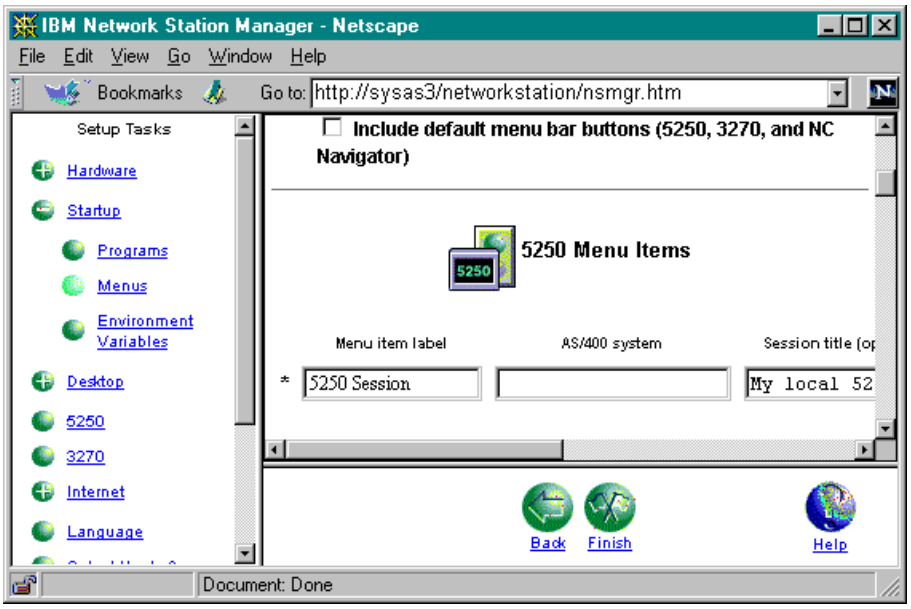


Figure 127. Customize System Default Menu Bar Buttons

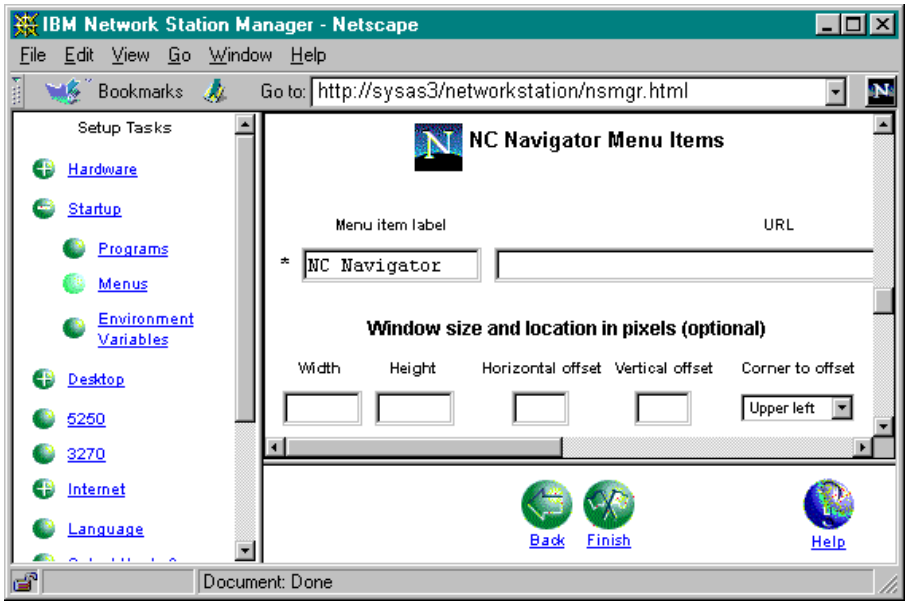


Figure 128. Add Custom NC Navigator Button to System Default Menu Bar

2. The group profile must already exist to set group preferences. Therefore, create the group profile grp3270 and a dummy user ID (which references grp3270 in its profile) on the *master copy* system, SYSAS3.

   Note: The grp3270 profile is a normal AS/400 group profile.

   Use the IBM Network Station Manager to add a 3270 button to the Menu Setup Task for the group grp3270 as shown in Figure 129.

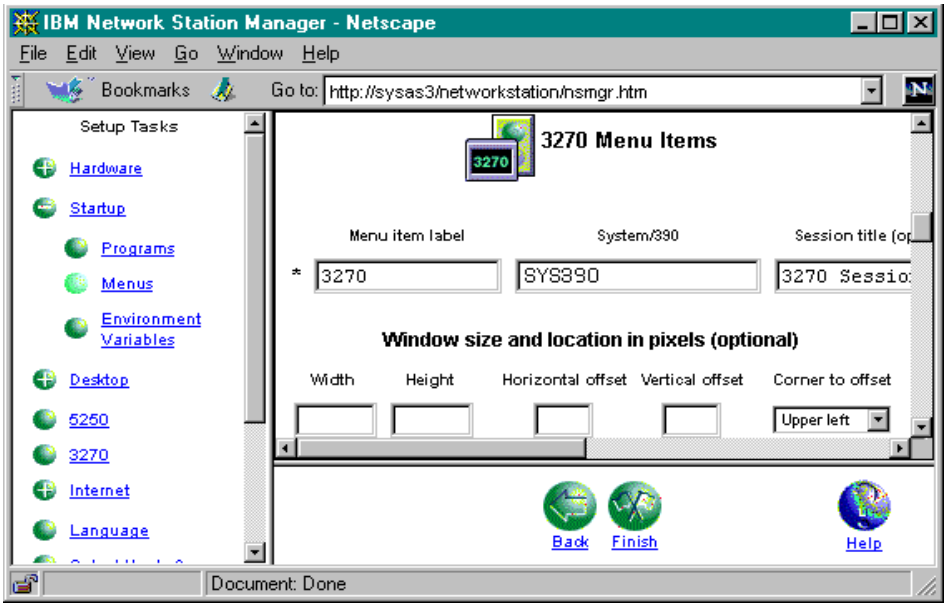


Figure 129. Add 3270 Menu Bar Button to Group Grp3270's Preference Settings

3. On the central SYSAS3 AS/400 system (source system), run the following command to create a *save file* which will contain the IBM Network Station Manager for AS/400 product and its installed PTFs. (In our environment, no one was actively using Network Station Manager when we performed this step.)

   ```
   CRTSAVF FILE(WORKLIB/C05SAVF) TEXT('savf for savlicpgm of 5648C05')
   ```

4. On the central SYSAS3 AS/400 system, run the following command to *save* the IBM Network Station Manager for AS/400 product to the previously created save file.

   ```
   SAVLICPGM LICPGM(5648C05) DEV(*SAVF) SAVF(WORKLIB/C05SAVF)
   TGTRLS(*CURRENT)
   ```

From the central SYSAS3, use the following commands to FTP the C05SAVF containing the 5648-C05 product to the existing as4work library on the remote server SYSAS4:

```
ftp sysas4
(Enter user ID and password when prompted.)
bin
cd /QSYS.LIB/as4work.lib/
lcd worklib
put c05savf
```

5. On the target system (the remote server SYSAS4), run the following command:

   ```
   RSTLICPGM LICPGM(5648C05) DEV(*SAVF) OPTION(*BASE) RSTOBJ(*ALL)
   SAVF(AS4WORK/C05SAVF)
   ```

   You should see messages similar to the following near the bottom of your job log, indicating a successful installation.

   ```
   Object moved.
   Object moved.
   Object moved.
   Object moved.
   Object moved.
   Object QAYTCSNC1P in QUSRSYS type *FILE created.
   1 objects duplicated.
   Ownership of object QAYTCSNC1P in QUSRSYS type *FILE changed.
   Object STRNSSA in QSYS type *CMD deleted.
   Object STRNSSA in QSYS type *CMD created.
   1 objects duplicated.
   Ownership of object STRNSSA in QSYS type *CMD changed.
   Object QAYTCSNC1 in QUSRSYS type *FILE created.
   1 objects duplicated.
   Ownership of object QAYTCSNC1 in QUSRSYS type *FILE changed.
   File QAYTCSNC1P started journaling to journal QYTCSJRN.
   Migration program completed successfully.
   *LNG objects for NLV 2924 for product 5648C05 option *BASE release
   *FIRST restored.
   Objects for product 5648C05 option *BASE release *FIRST restored.
   ```

6. On the remote server, run the Network Station Setup Assistant (STRNSSA) command to start the Network Station Setup Assistant. Go through *each* task and sub-task as appropriate, even though the *Completed* column may indicate a status of *YES*.

   Note: If you receive a message in your job log indicating that *task 5000 failed .... port 80 was not active*, start the HTTP server DEFAULT instance by running the following command and then trying *task 5000* again.

```
STRTCPSVR SERVER(*HTTP) HTTPSVR(DEFAULT)
```

7. Because the central AS/400 SYSAS3 system was used to create the *master* system wide default preferences and the grp3270 group preferences, these configuration files must be transferred to the remote boot server from the *master* SYSAS3.

8. Although Windows Explorer can be used to drag and drop whole IFS directories from one AS/400 system to another, in this case, we decided to save all of the files in the path */QIBM/UserData/NetworkStation/* and then FTP them to the remote server.

   Note: Alternatively, if you know which files are affected and there are only a few of them, FTP the specific configuration files instead.

   On the source system, after creating a group's save file in the WORKLIB library, run the following command to *save the files* in the */QIBM/UserData/NetworkStation* IFS path to the save file:

   ```
   SAV DEV('/QSYS.LIB/WORKLIB.LIB/groups.file')
   OBJ(('/QIBM/UserData/NetworkStation/*')) DTACPR(*YES)
   ```

   On the source system, start an FTP session to the target system and then use the following commands to transfer the IFS files to a save file in the existing library as4worklib:

   ```
   bin
   cd /QSYS.LIB/as4work.lib/
   lcd worklib put groups
   ```

   On the target system, issue the following command to restore the files:

   ```
   RST DEV('/QSYS.LIB/as4work.lib/groups.file')
   OBJ(('/QIBM/UserData/NetworkStation/*')) ALWOBJDIF(*ALL)
   ```

   If the desired group profile (such as grp3270) does not already exist on the target system, create the group profile now. For users on the SYSAS4 (target) system to utilize the group preferences, their user profiles on that target system *must* have the group profile named in the *GRPPRF* field.

9. Ensure that the DHCP server options are set up correctly on SYSAS1 so that the IBM Network Stations in Rochester have SYSAS4 system defined as their base code server. For example, option 66 needs to point to different TFTP servers to allow the IBM Network Stations in different remote sites to obtain their base code from the appropriate server. For more details on DHCP configuration, refer to the manual, *IBM Network Station Manager Installation and Use,* SC41-0664, and *TCP/IP Configuration and Reference*, SC41-5420, which are online respectively at the Web sites: www.ibm.com/nc/pubs and www.as400service.ibm.com

In addition, the *AS/400 TCP/IP Autoconfiguration: DNS and DHCP*, SG24-5147, is available online at: www.redbooks.ibm.com

As a result of the previous steps, the IBM Network Station users at the Rochester remote site boot from their *local* SYSAS4 AS/400 system which was *replicated* from the *master copy* SYSAS3 AS/400 system at the central site. Because preference files were copied from SYSAS3 to SYSAS4, all IBM Network Station users in the Rochester location see a default desktop that contains the custom 5250 and NC Navigator menu bar buttons. In addition, users who are members of the grp3270 l also see a 3270 button on their IBM Network Station desktop.

7.3 Summary

The information in this chapter includes *as-is*, non-supported techniques for replicating an IBM Network Station Manager Release 3 environment from one AS/400 to another when implementing multiple AS/400 boot servers. In review, some crucial tasks when using one of the replication techniques in this chapter are:

- Develop an implementation plan and draw or revise a network diagram.
- Determine whether the Release 3 separation of servers function will be used. For example, will you be using a central server for authentication and the remote sites for base code serving or will each remote server fulfill the authentication, terminal configuration and base code server roles? If you are using DHCP, consider the location of the server. Also, there may be a requirement to install multiple DHCP servers. Refer to the manual, *TCP/IP Configuration and Reference*, SC41-5420.
- Review the desktop customizing needs of the remote users. If the remote servers are providing the authentication server function, are there certain system level, group, or even user defaults which can be set on the *master copy* so that these preferences can be replicated initially to all remote AS/400 boot servers?
- Are the remote servers and the source *master copy* system at the same OS/400 levels? The techniques in this chapter were tested in an environment where both the source and the target systems were at V4R3. If they are not at the same level, ensure that you verify that pre-requisite PTFs are installed as directed in the previous sections. In addition, the steps involving the saving of products or files must reflect the proper target release level.
- If using these replication techniques, please test them in your own environment before using them to create production systems.

Chapter 8. Using a Network Station to Access Mail

Electronic mail, called e-mail, is information that is sent electronically to and from users on an interconnected network by using a computer with special application software.

In this chapter, we describe how the IBM Network Station can access e-mail from POP3 Server and Domino Server.

8.1 POP3 Mail Configuration

The Post Office Protocol (POP) is the AS/400 implementation of the Post Office Protocol Version 3 mail interface. This server allows AS/400 systems to act as a POP server for any clients that support the POP mail interface.

The POP3 Server is a simple store-and-retrieve mail system which manages temporary electronic mailboxes for the POP3 users' mail. The mail is stored until the client retrieves it from the mail box. If the client configuration specifies the delete option, the mail items is deleted as they are retrieved. The mail remains in its original form (ASCII) while it is stored on the AS/400 system acting as the POP3 server.

8.1.1 Basic POP3 Configuration

Use the following steps to perform the basic configuration that you need to deliver mail to and from POP3 clients:

1. To configure the AS/400 SMTP serve, use these steps:
   a. Configure the host name and domain name using the Change TCP Domain (CHGTCPDMN) command or Configure TCP/IP (CFGTCP) command, menu option 12 (see Figure 130).

```
                    Change TCP/IP Domain (CHGTCPDMN)

Type choices, press Enter.

Host name  . . . . . . . . . . .   'AS1'

Domain name  . . . . . . . . . .   'MYCOMPANY.COM'

Host name search priority  . . .   *REMOTE       *REMOTE, *LOCAL, *SAME
Domain name server:
  Internet address . . . . . . .   '10.1.1.1'
```

Figure 130. Option 12 of the CFGTCP Menu - Change TCP/IP Domain

© Copyright IBM Corp. 1999

b. Verify that there is an IP address associated with the host name for the system, either in the DNS server configuration or local host table.

   For the DNS server, add an **A** record in the DNS server configuration for the SMTP mail server host as shown in the following example:

```
DNS
as1.mycompany.com IN A 10.1.1.1
```

Figure 131. DNS Server Configuration

   For the local host table, use the Add TCP Host Table Entry (ADDTCPHTE) command or Configure TCP/IP (CFGTCP) command, menu option 10 to add the host's IP address. The host table entry is shown in Figure 132.

```
                      Display TCP/IP Host Table Entries
                                                              System:
 Internet Address . . . . . . . . . . . . :   11.3.1.283
 Host names:
   Name . . . . . . . . . . . . . . . . . :   ASM0719.MYCOMPANY.COM
```

Figure 132. Display of Host Table Entry

2. Add an entry in the system distribution directory for the user. Use the Work with Directory Entry command, `WRKDIRE` ,and then select menu option **1**. Figure 133 shows the display with only the relevant parameters.

```
                            Add Directory Entry

Type choices, press Enter.

  User ID/Address . . . .   USER1     AS1
  Description . . . . . .   Pop3 User
  System name/Group . . .   AS1                   F4 for list
  User profile  . . . . .   USER1                 F4 for list
  Network user ID . . . .   USER1
```

Figure 133. Directory Entry for POP User - General Information

Figure 133 on page 226 shows the first display for adding a new directory entry. From this first display, page down 3 times to get to the display as shown in Figure 134 on page 227.

```
                          Add Directory Entry

Type choices, press Enter.

  Mail service level  . .   2                    1=User index
                                                   2=System message store
                                                   4=Lotus Domino
                                                   9=Other mail service
    For choice 9=Other mail service:
      Field name  . . . .                          F4 for list

  Preferred address . . .   3                    1=User ID/Address
                                                   2=O/R name
                                                   3=SMTP name
                                                   9=Other preferred address
    Address type  . . . .                        F4 for list
    For choice 9=Other preferred address:
      Field name  . . . .                          F4 for list
```

Figure 134. Mail Service Level - System Message Storage (Preferred Address)

On the display, as shown in Figure 134, press **F19** to configure the SMTP name for the user. The display in Figure 135 appears.

```
                          Add Name for SMTP
                                                          System:
Type choices, press Enter.

  User ID . . . . . . . . :   USER1
  Address . . . . . . . . :   AS1



  SMTP user ID  . . . . . .   user1
  SMTP domain . . . . . . .   as1.mycompany.com




  SMTP route  . . . . . . .
```

Figure 135. Add Directory Entry - SMTP Name for User

3. To start the applicable mail servers on the AS/400 system, use the following steps:

   a. To start the SMTP server, run the following command:

      ```
      STRTCPSVR SERVER(*SMTP)
      ```

b. To start the POP3 server, run the following command:

```
STRTCPSVR SERVER(*POP)
```

c. To start the Mail server Framework, run the following command:

```
STRMSF
```

For more detail information about how to configure the POP3 Server on an AS/400 System, refer to the redbook *AS/400 Electronic-Mail Capabilities,* SG24-4703. This manual is available at the Web site: www.redbooks.ibm.com

The term POP or POP3 is used throughout this chapter and should be considered synonymous.

8.2 Lotus eSuite Workplace

Lotus eSuite Workplace is an all-Java business application suite which provides users with an interactive desktop that includes the following functions:

- Web-browser
- Word processor
- Spreadsheet
- Presentation graphics
- Calendar
- Address book
- e-mail client

The eSuite mail applet is a lightweight e-mail client, designed for Internet environments, that supports standard messaging formats and open protocols. It provides a complete, easy-to-use solution for reading and composing mail messages.

Please read *Implementation of Lotus eSuite WorkPlace for IBM Network Station for AS/400*. This documentation can be obtained from the Web site: http://service.boulder.ibm.com/nc/as400

These *readme* files contain detailed information about installing Lotus eSuite Workplace on the AS/400 system. In addition, a redbook pertaining to Lotus eSuite Workplace is planned for 1999.

Note

A IBM Network Station Series 1000, with 64MB of memory, is required for Lotus eSuite Workplace.

Figure 136 on page 229 shows the main Lotus eSuite Workplace desktop.

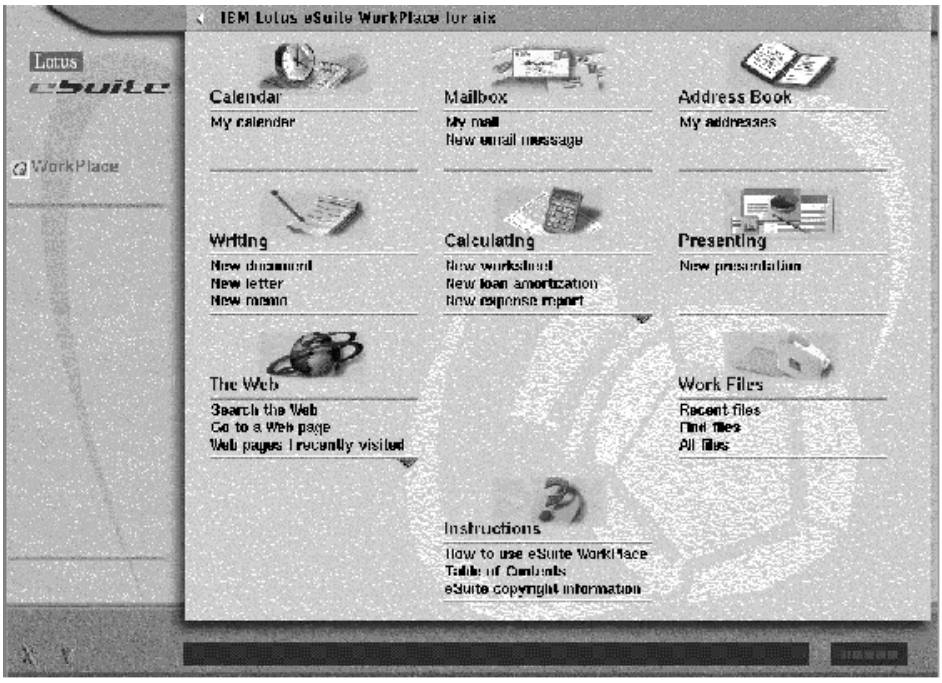


Figure 136. eSuite Workplace Desktop

8.2.1 Starting eSuite on the Network Station

To enable users to start eSuite, perform the following tasks:

1. Enable users or groups to access eSuite.
2. Start RMI and eSuite registry server on the AS/400.

8.2.1.1 Enabling Users or Groups to Access eSuite

Before users or groups can access eSuite, the system administrator must enable these users or groups to use eSuite.

To enable users, sign on to the IBM Network Station Manager with an administrative level user ID and complete the following steps:

1. Click **Startup** and then **Menus** on the left side of the display. The Menu Contents Default display is shown (see Figure 137).

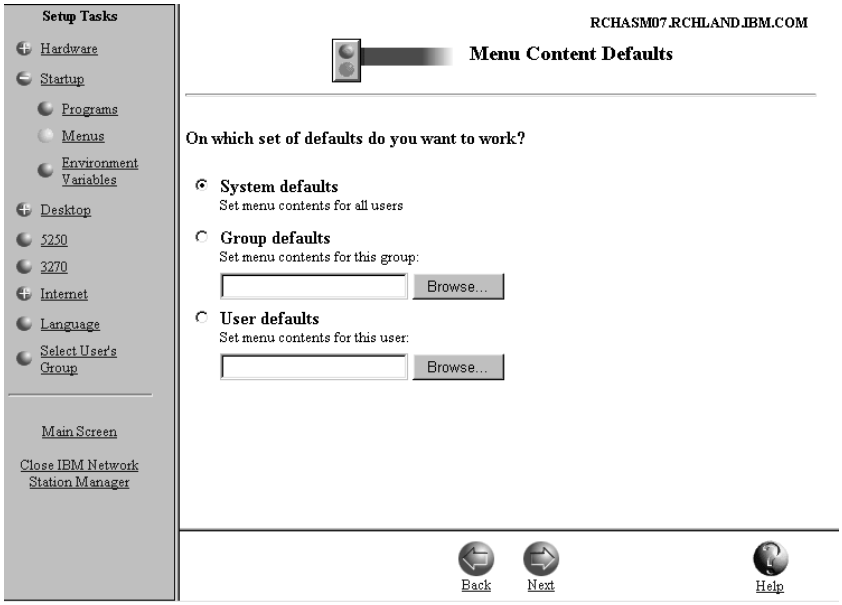


Figure 137. Menu Content Defaults Display

2. Click **Group defaults** or **User defaults** depending on which group or user you want to enable and then click **Browse**.
3. Select the group or user you want to enable, then click **Select** and **return**.
4. Click **Next** at the bottom of *Menu Content Defaults*, this shows you the *Menu Content* for the group or user you wish to enable.
5. The next display is the *Desktop and Menu Bar options*. Click the **Desktop style** field and select **Lotus eSuite Workplace without menu bar** or **Lotus eSuite Workplace with menu bar**.
6. Click **Finish** to save the preferences.

The eSuite Workplace loads automatically every time the designated group or user logs in to their Network Station. Figure 136 on page 229 appears if the logon completed successfully.

Note

If the user or group does not receive the main Lotus eSuite Workspace desktop, after logging on to the Network Station, ensure that both the RMI and eSuite servers are active on the AS/400. These jobs, QESRRMI and QESRSVR, run in the QSYSWRK subsystem. Details on starting these servers are included in the following section.

8.2.1.2 Starting RMI and eSuite Registry Server from AS/400 System

The RMI and eSuite Registry servers run on the AS/400 system and must be started before starting the eSuite Workplace on your Network Station.

To start the RMI and eSuite registry servers, run the following command at an AS/400 command prompt:

```
QESUITE/STRESRSVR
```

A message indicating the eSuite registry server has started is sent to the QSYSOPR message queue. The message is shown in Figure 138.

```
                          Display Messages
                                                        System:
Queue . . . . . :   QSYSOPR               Program . . . . :   *DSPMSG
  Library . . . :     QSYS                  Library . . . :
Severity  . . . :   90                    Delivery  . . . :   *HOLD

Type reply (if required), press Enter.
  Adapter has inserted or left the ring on line TRNLINE.
  Adapter has inserted or left the ring on line TRNLINE.
  Adapter has inserted or left the ring on line TRNLINE.
  eSuite registry server (014486/QESUITE/QESRSVR) starting.
```

Figure 138. QSYSOPR Message Queue Showing Start of eSuite Server

8.2.2 eSuite Mail Configuration on Network Station

This section describes how to setup and configure eSuite mail on the Network Station to access POP3 Server on the AS/400 system.

1. To access eSuite mail, click **My mail** under *Mailbox* in the eSuite Workplace. The following display is shown (see Figure 139 on page 232).

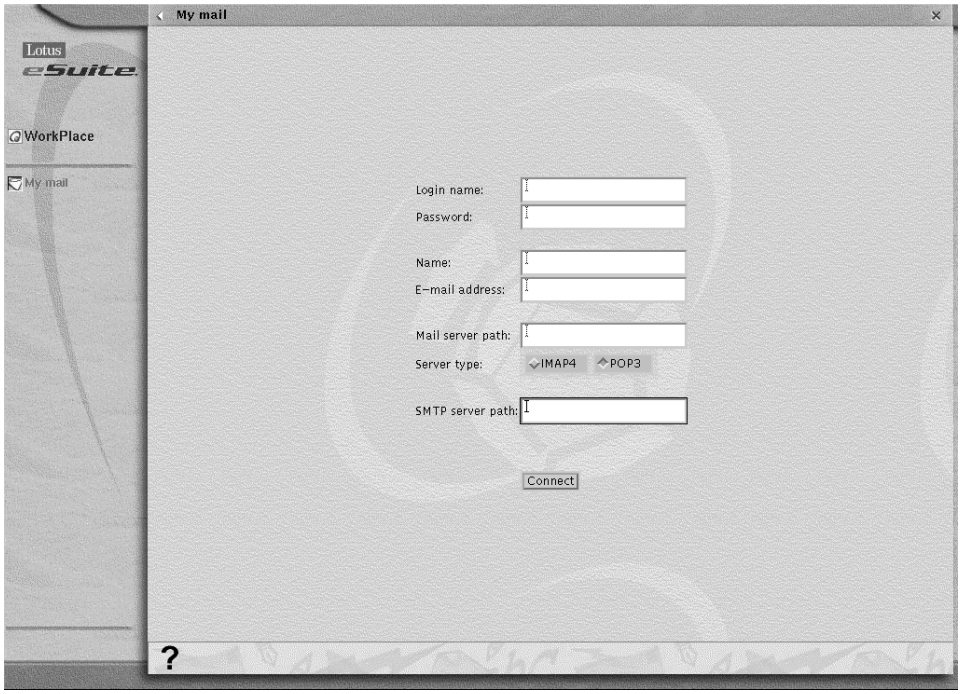


Figure 139. eSuite Mail Configuration

2. The first time you start eSuite mail, you are prompted to enter some information. Ask your system administrator for the following login information:

   - **Login name.** For example, if you are John Doe, your login name to your eSuite mail account might be *jdoe*
   - **Mail account password.** For example, your password is: *lotus*.

     Note: The asterisk (*) character is shown when you type in your password.
   - **Name.** Enter your full name here or as you would like it to appear to the mail recipient. For example, if your full name is John B. Doe, you can enter *John Doe* or any other combination.
   - **e-mail address.** This is the e-mail address that your mail recipients see when they receive your messages. For example, if you are John Doe, your e-mail address might be: *jdoe@sysnam.mycompany.com*. In this example, the AS/400 host name is *sysnam*, the domain name is *mycompany.com*., and *jdoe* is the AS/400 profile name for the user on the AS/400 system.

- **Mail server path.** This is the path to the mail server where your messages are stored, for example: *sysnam.mycompany.com*
- **Mail server type (IMAP4 or POP3).** This identifies the mail server type to which you are going to login. In this case, click **POP3** instead of *IMAP4*.
- **SMTP server path.** This is path to the SMTP server that sends your messages over the Internet. For example: *sysnam.mycompany.com.* In this example, we use the same AS/400 system as both our POP3 and SMTP server.

After you enter your login information, click **Connect to start eSuite mail**. Figure 140 shows the eSuite Inbox.

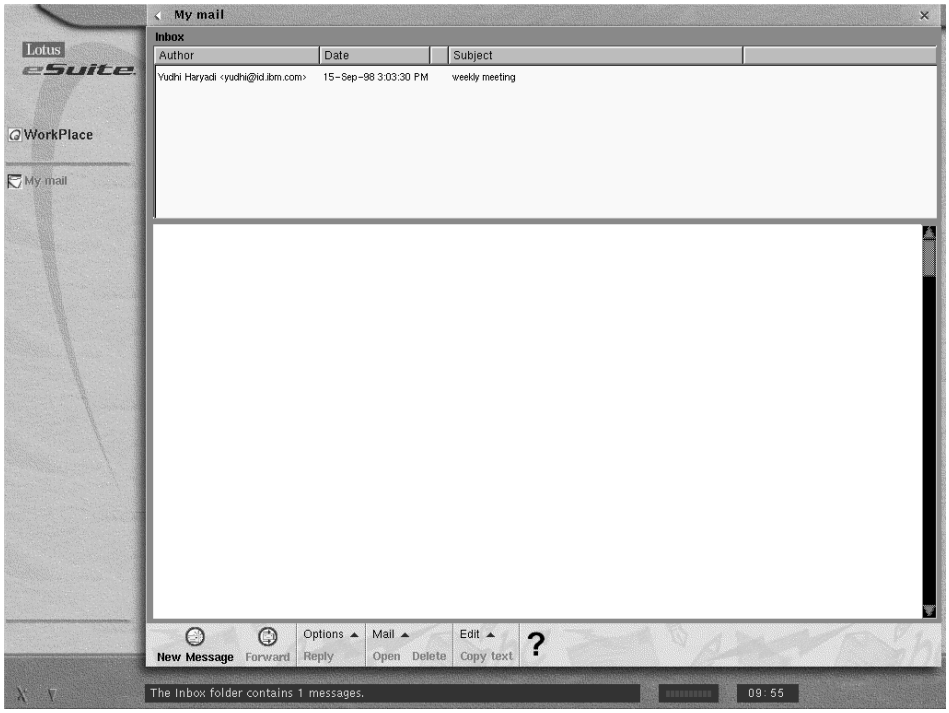


Figure 140. eSuite Inbox

Tip

You can set eSuite mail to automatically log the user into the mail account using the *user name* and *password* from the initial login. Follow these steps to accomplish this:

1. In the action bar at the bottom of the display, click **Mail**.
2. In the pop-up menu, click **Preferences**.
3. In the pop-up-display, click **Management**.
4. Click one or more options:
   - Move deleted messages intothe *Trash* folder.
   - Always save a copy of a message when sending mail.
   - Automatically add author to address book when opening mail message.
   - Skip mail login (save user name and password)
5. Click **OK**. Your changes take effect immediately.

8.3 NC Navigator Access

NC Navigator mail has many capabilities to help you read and manage E-mail messages. These functions are available by clicking various pulldown options from the NC Navigator Mail menu bar. This section describes how to configure and setup the NC Navigator to access the POP3 server on the AS/400 system.

8.3.1 Starting NC Navigator

To start NC Navigator on your Network Station, you must perform the following tasks:

1. Configure proxy.
2. Load NC Navigator on the *from* Network Station.

8.3.1.1 Configure Proxy

Use the following steps to configure a Proxy within the IBM Network Station Manager:

1. Before you can use NC Navigator to surf the Internet, sign on to IBM Network Station Manager with a user ID that has administrator authority.
2. On the left side of the display, click **Internet —> Network**. Select **System Defaults** for all users.

3. Click **Next** at the bottom of the display. The Network Setting display appears as shown in Figure 141.

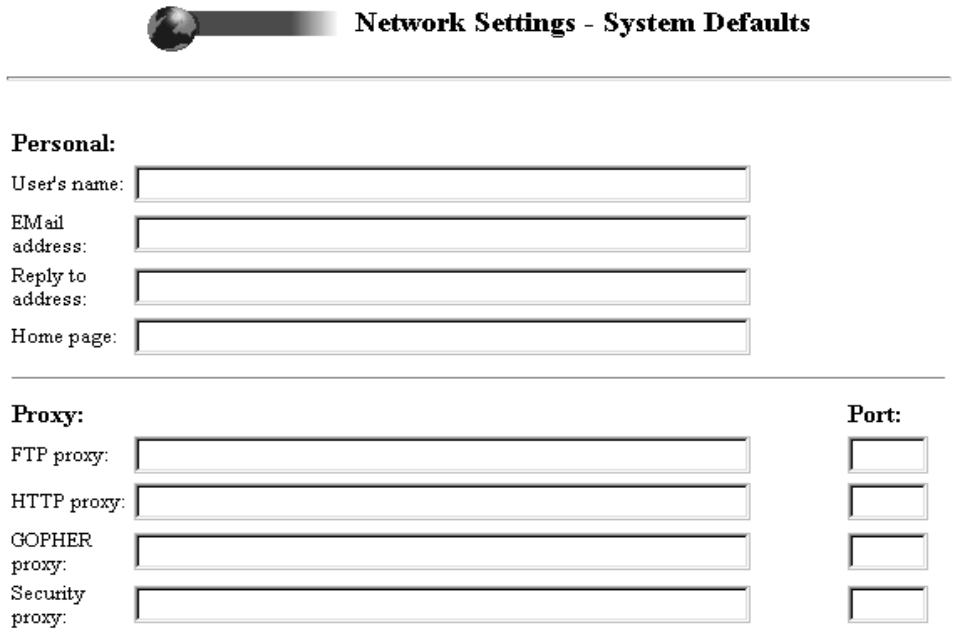


Figure 141. Network Settings - System Defaults Display

4. Enter the **HTTP Proxy address** and **Port number**.
5. Click **Finish** to end and save configuration.

8.3.1.2 Loading NC Navigator from Network Station

Use the following steps to load the NC Navigator on the IBM Network Station:

1. Logon to the Network Station.
2. After the login is complete, clicks **NC Navigator** on the menu bar.

   After a few moments, the NC Navigator display is shown. An example of this display is shown in Figure 142 on page 236.

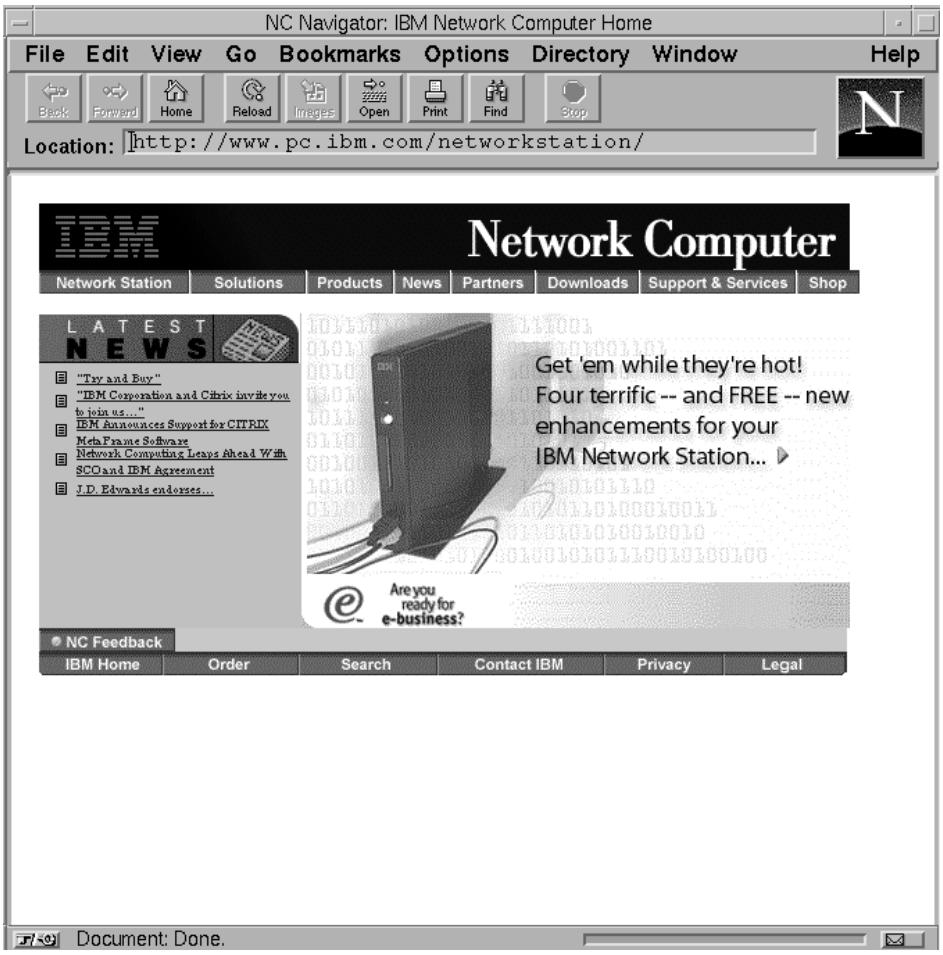

NC Navigator: IBM Network Computer Home
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Reload Images Open Print Find Stop
Location: http://www.pc.ibm.com/networkstation/
Network Computer
Network Station Solutions Products News Partners Downloads Support & Services Shop
LATEST NEWS
"Try and Buy"
"IBM Corporation and Citrix invite you to join us..."
IBM Announces Support for CITRIX MetaFrame Software
Network Computing Leaps Ahead With SCO and IBM Agreement
J.D. Edwards endorses...
Get 'em while they're hot! Four terrific -- and FREE -- new enhancements for your IBM Network Station...
Are you ready for e-business?
NC Feedback
IBM Home Order Search Contact IBM Privacy Legal
Document: Done.

Figure 142. Main Dsplay of the NC Navigator Browser

8.3.2 Configuring NC Navigator to Access e-mail

Before you can access e-mail using the NC Navigator, you must first setup the e-mail configuration.

Use the following steps to configure e-mail:

1. Select the **Mail** options.
2. Set up server information.
3. Set up your identity.

8.3.2.1 Selecting Mail Options

The first time you start NC Navigator mail, you may need to enter some information.

1. From NC Navigator display, click **Options —> Mail and News Preferences.**
2. Click the **Servers** tab. The display in Figure 143 is shown.

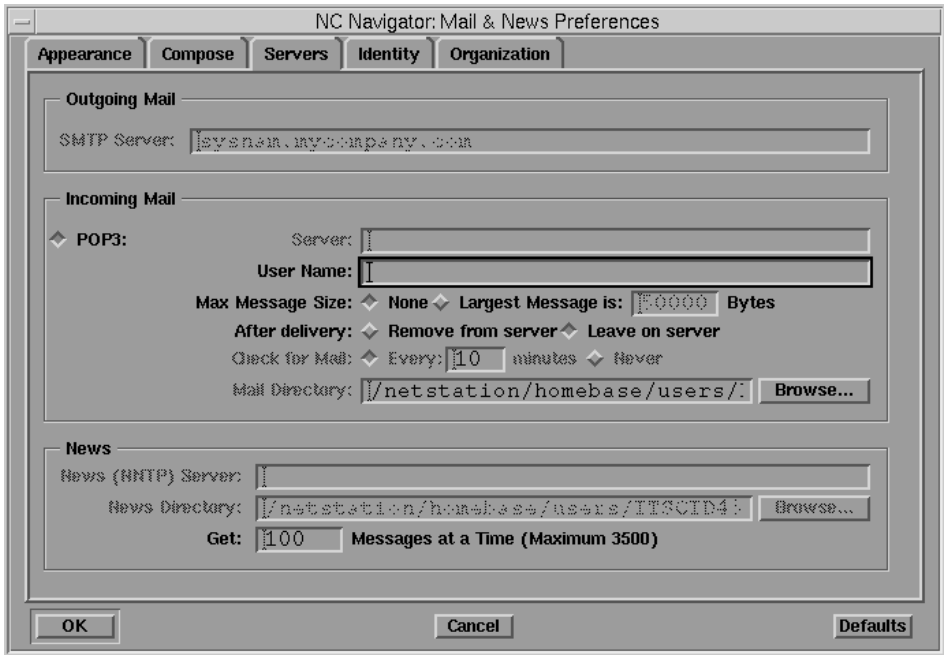


Figure 143. NC Navigator: Mail & News Preferences Display

3. To access e-mail on POP3 server, you must provide the server information. As shown in Figure 143, enter the following information:
   - **SMTP Server**—For example: *sysnam.mycompany.com*. If the field is disabled, ask your system administrator to enter it using IBM Network Station Manager. In this example, *sysnam* is the SMTP server that runs on the AS/400 and the domain name is *mycompany.com.*
   - **POP3 Server**—For example: *sysnam.mycompany.com*. In this example we use the same AS/400 system for both the SMTP and POP3 server.
   - **User Name**—For example: *jdoe*.
4. To allow your mail recipient to see your identity on incoming e-mail messages, click on **Identity** tab, and enter the information:

- **Name**—This is the name that your mail recipient will see when they receive your message.For example: *John Doe*,
- **Email Address**—For example: *jdoe@sysnam.mycompany.com.* In this example, *jdoe* is the AS/400 profile name for the user on the AS/400 system. The AS/400 host name is *sysnam* and the domain name is *mycompany.com*.

An example of the NC Navigator mailbox is shown in Figure 144.

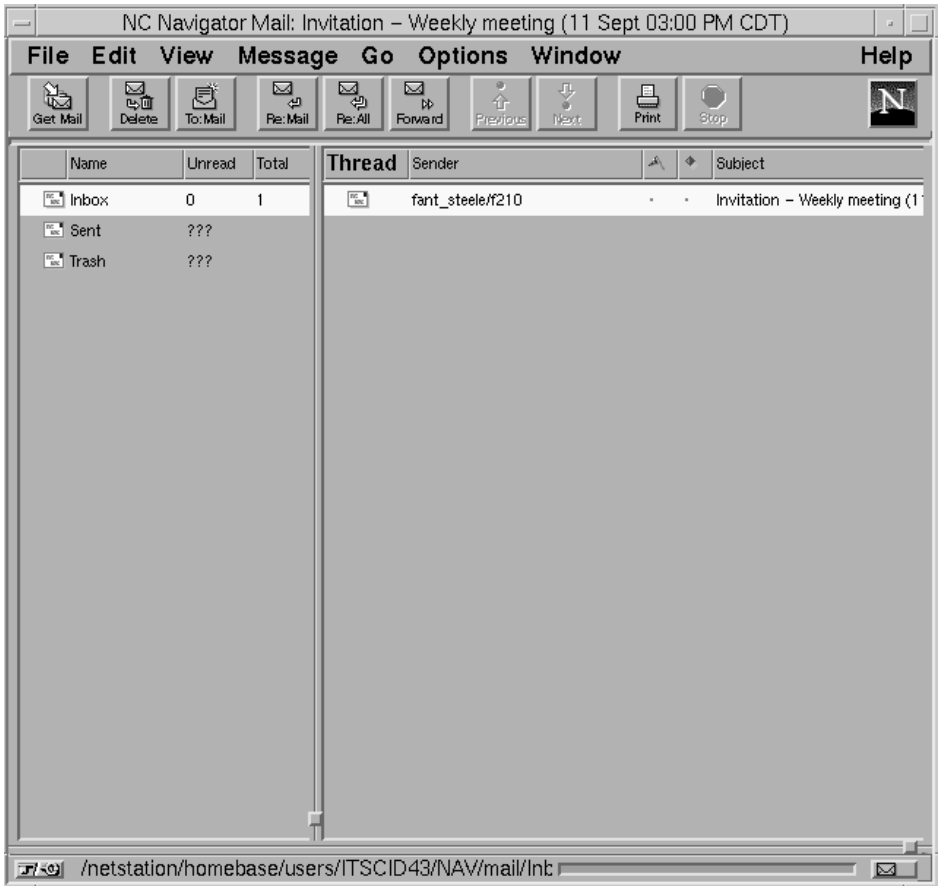


Figure 144. NC Navigator Mail Inbox

8.4 Domino Access

Domino for AS/400 is the implementation of a Lotus Domino server on the AS/400 platform. Lotus Domino, on any of the supported platforms, can provide users with a range of server functions.

Some of these server functions are:

- Mail server for Notes, POP3, or IMAP4 clients
- Database server
- Database replication server
- HTTP server

In providing these server functions, Domino supports many protocols. These protocols include:

- For messaging, Domino supports: Post Office Protocol 3 (POP3), Internet Message Access Protocol (IMAP), Lightweight Directory Access Protocol (LDAP), Simple Mail Transfer Protocol (SMTP), and Multipurpose Internet Mail Extension (MIME).
- For Web use, Domino supports: Hyper Text Transfer Protocol (HTTP), Hyper Text Markup Language (HTML), and Network News Transfer Protocol (NNTP).

To allow Notes clients or Web browsers to connect to a Domino server running on the AS/400 system, the OS/400 TCP/IP support must be configured and started. Therefore, TCP/IP Connectivity Utilities product must be installed on your AS/400 system.

This section describes how the Domino server, on the AS/400 system, can be assessed by an IBM Network Station user though the NC Navigator browser or by using the X11 or ICA protocol to access a service running a multi-user implementation of NT (such as, Microsoft Windows NT Server 4.0, Terminal Server Edition and Citrix MetaFrame).

8.4.1 Deciding What to Specify for Server Characteristic

When you set up the first Domino server, you must provide information that defines the key characteristics of the server. These characteristics include:

- The name of the server
- The location of the server's data directory
- The name of your organization
- Details about the person who is the server administrator

Before you run the Configure Domino Server (CFGDOMSVR) command, decide what to use for these key characteristics. These characteristics are discussed here briefly. For more information, see *Planning the Domino System.*

8.4.1.1 Server Name

To avoid additional TCP/IP configuration, use the TCP/IP host name of your AS/400, as the Domino server name.

Each Domino server has a unique name that is maintained in its own ID file. Domino creates the server ID automatically during the server setup processing.

8.4.1.2 Data Directory

The data directory contains files used by the Domino server and users of the server. On a PC-based platform, the data directory typically has the directory path:

```
x:\notes\data
```

The *x* is the drive letter. On the AS/400 system, the files are stored in the integrated file system, which supports a directory structure similar to DOS or Windows. To make the path easy to remember, specify a similar directory path on the AS/400 system. For example:

```
/notes/data
```

Notice that a forward slash (/) is used to specify a path in the AS/400 integrated file system.

Each server must have its own data directory. Therefore, if you set up more than one Domino server (partitioned servers) on your AS/400 system, use a unique directory path for the second and subsequent servers. For example:

```
/servername/notes/data
```

The *servername* is the name of the second or subsequent Domino server.

Note

If you use an existing directory as the data directory, make sure that you set up the necessary authorities to the directory. The QNOTES user profile must have *RWX data authority as well as *OBJEXIST and *OBJMGT object authority to the directory. The owner of the data directory and subdirectories must have *OBJEXIST and *OBJMGT authority to the directory.

8.4.1.3 Organization

Typically, the organization name is the name of your company or a major division within your company.

Each organization has a Certifier ID that is stored in a file named CERT.ID. During the server setup processing, Domino creates the organization Certifier ID automatically using the organization name you specify and an optional country code. When you register new users or servers, Domino uses the Certifier ID to certify each user or server. You also use the organization Certifier ID when you create organizational unit certifiers for a hierarchical name scheme.

8.4.1.4 Administrator

The administrator can perform operations, on the Domino server, such as starting and stopping the Domino server. Although you only need to provide a last name, use a first name and, if needed, a middle initial to ensure that the administrator's name is unique. It is very important that you remember and record the name and password that you specify for the administrator. Domino creates a user ID for the administrator during the setup processing.

Some Domino server options are not automatically set up for you. As a result, you must request these options through fields in the Configure Domino Server (CFGDOMSVR) command. For example:

- **Web browser**

  Use this option to set up the HTTP Web server. If you enter ***HTTP** in this parameter, the Web server feature automatically starts the Domino HTTP server and enables Web browser access to the Domino server.

- **Internet mail packages**

  Use this option to set up mail support such as POP3 or SMTP/MIME MTA.

- **Advanced services**

  If you installed the Domino Advanced Services, use this option to include one or more Advanced Services features such as setting up the Domino server as a partition server or as part of a server cluster.

Refer to *Lotus Domino for AS/400, Installation, Customization, Administration,* SG24-5181*,* for detailed information about configuring Domino on the AS/400 system. You can find additional information on the Web site at: www.as400.ibm.com/notes

8.4.2 Avoiding Conflicts between AS/400 HTTP Server and Domino

The AS/400 operating system (OS/400) includes several TCP/IP application servers, including an HTTP server, that is known as the Internet Connection Secure Server (ICS). This HTTP server processes HTML documents, CGI scripts, and Java scripts for home pages. Domino for AS/400 also provides an HTTP server capability which enables Notes databases to be seen as HTML documents on the Web.

You can have both HTTP servers installed and running. However, the Domino HTTP server and the Internet Connection Secure Server are both set up to use TCP/IP port 80. Because both HTTP servers use the same port, the server that is started second will have a problem accessing the port. To eliminate this problem, do *one* of the following:

- End TCP/IP HTTP server by entering the following AS/400 command:

  ```
  ENDTCPSVR *HTTP
  ```

  Then use the AS/400 Work with HTTP Configuration (WRKHTTPCFG) command to change the TCP/IP server to allow it to use a port other than port 80.

Note

If a port number other than 80 is used, the port number must be specified if accessing the IBM Network Station Manager from a browser or from NC Navigator on the IBM Network Station. For example, if port 9999 has been set in the HTTP configuration, the URL that can access the IBM Network Station Manager is: http://sysipadr:9999/networkstation/admin

The *sysipadr* is the IP address of the AS/400 system that has the IBM Network Station Manager installed.

- Alternatively, change the Domino HTTP server to allow it to use a port number other than port 80. You change the HTTP server port number in the server document for the Domino server.

Note

If you set a port number other than 80, the client must include a specific port number on requests to the Domino server. The port number is preceded by a colon and follows the host name in the URL. In this example we use port 8080 for Domino HTTP server, the URL, http://as1.mycompany.com:8080/, requests the default page from a host named *as1.mycompany.com* that is listening on port 8080. The AS/400 system on which the Domino server is installed and running is *as1*.

For more information, refer to the manual I*nternet Connection Services and Internet Connection Secure Server for AS/400 Webmasters Guide*, GC41-5434. Notice that with V4R3, the ICS product was renamed to IBM HTTP Server for AS/400.

8.4.3 Accessing the Web Browser

In addition to the Notes Mail template (MAIL46.NTF) that ships with Domino 4.6.2 for AS/400, Lotus also supplies two additional Mail templates that allow increased functionality to a Domino Mail file when being accessed by a Web browser. The two templates are called WebMail (MAILW46.NTF) and combined Mail (MAILC46.NTF).

The WebMail templates are designed for the Domino Mail user that is using a Web browser such as Microsoft Internet Explorer, Netscape Navigator or NC Navigator. For example, these users may include a Client Access user or an IBM Network Station user accessing Domino through the NC Navigator Web browser.

The combined Mail template is designed for the mail user who needs to access their Domino Mail using a Notes client and a browser. Both templates provide access to the integrated Mail, Calendaring & Scheduling and Task Management features provided on the Domino Mail Server.

8.4.3.1 Setting Up Web Mail for Web Users

You can set up mail for Web users on a Domino server. Web mail is a mail database created with either the MAILW46.NTF or MAILC46.NTF mail template. Follow these steps to setup mail access for Web users:

1. Ensure the Domino server is set up as a Web server running the HTTP server task.
2. Ensure you have registered the user on the server and select **Set Internet Password** to set an Internet password in the *Person Document*.

3. In the *Public Address Book*, open the **Server** document for the Web server. In the *Agent manage***r** section, enter the name of a person or server in the **Run restricted LotusSript agents** field. This person or server is anyone you want to have this access on the server, and whose ID to which you have access. It is not necessarily the name of the Web use because the user does not have a Notes ID.
4. Start the Notes workstation and switch to the ID specified in step 2.
5. From the administration display, do the following steps to *sign* the templates using an ID allowed to run restricted LotusScript agents:
   a. Click **Database Tools**.
   b. Select **Sign a Database**.
   c. Click **Update existing signatures only**.
   d. Enter the template name in the *Filename* field and click **Sign**.
6. Create the database using one of the mail templates (MAILW46.NTF or MAILC46.NTF).
7. Add the name of the person or server from the ID specified in step 2 to the database access control list (ACL) of the mail file as a *designer*.
8. Add the Web user's name to the ACL as a **Manager** and change the Default access to **No Access**.
9. Change the *Maximum Internet name & password access* field in the *Advanced* tab on the ACL to **Designer**.
10. Change the default mail file in *Person Document* with the mail file that you created in step 5.

Every time you access the Domino server using a Web browser, it prompts you to enter a user name and password as shown in Figure 145 on page 245.

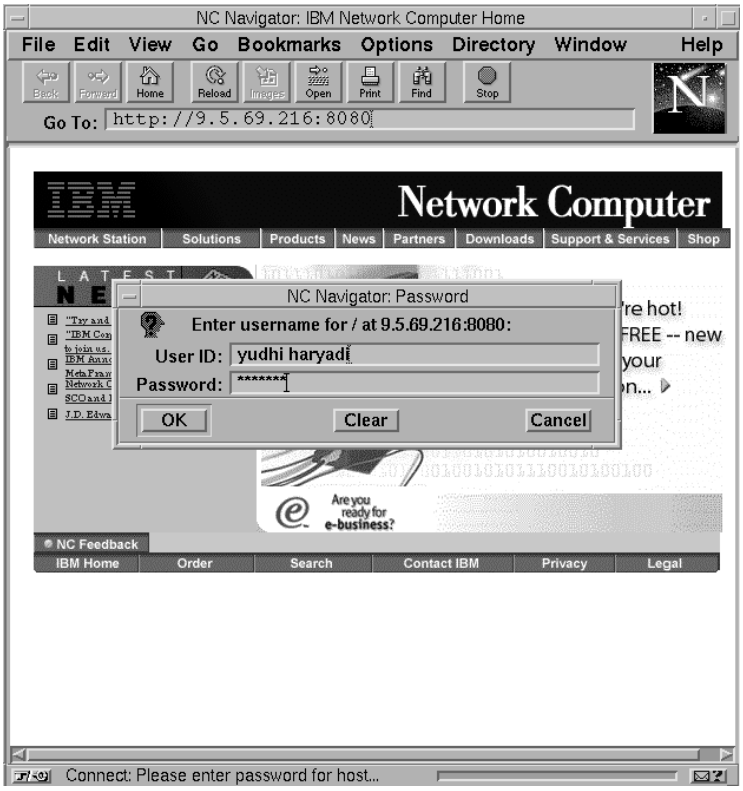

NC Navigator: IBM Network Computer Home
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Reload Images Open Print Find Stop
Go To: http://9.5.69.216:8080
Network Computer
Network Station Solutions Products News Partners Downloads Support & Services Shop
NC Navigator: Password
Enter username for / at 9.5.69.216:8080:
User ID: yudhi haryadi
Password: *******
OK Clear Cancel
Are you ready for e-business?
NC Feedback
IBM Home Order Search Contact IBM Privacy Legal
Connect: Please enter password for host...

Figure 145. User ID and Password Prompt

8.4.3.2 Views

User are presented with a full variety of Mail File views when accessing their WebMail templates. When using a browser to access the Mail file on the Domino Server, the user sees the views as shown in Figure 146 on page 246.

Figure 146. Views Display

These views are presented as icons on the left side of the window. Figure 147 on page 247 shows a sample Inbox view with a message visible on the right and other Views and Folders on the left.

Figure 147. Web Mail Inbox

The Web mail template uses the familiar Notes mail interface and contains many of the features found in the Notes mail template, including:

- Create messages and provide address information
- Create draft messages
- Create replies to messages
- Receive delivery reports for sent messages
- Specify a delivery priority and importance
- Organize messages in folders
- Create and view calendar entries and accept meeting invitations sent by others
- Look up free time for invitees

- Send broadcast meeting invitations
- Confirm, cancel, or reschedule meetings
- Review invitee responses
- Create and view bookmarks, phone messages, and tasks

Because of browser limitation, the following features are not yet available for Web mail users:

- Convert a mail message to a task
- Reply with history or forward documents
- Sign messages
- Schedule repeating appointments
- Reserve resources or rooms for a meeting
- Set and receive alarm notices
- Accept counter proposal for an RSVP
- Remove a person from an invitation list
- Delegate invitations to another person
- Counter propose invitation details
- Display tasks in the calendar view
- Enable and disable out of office agent
- Automatically accept invitations
- Add the sender of the memo to the Personal Address Book
- Choose letterhead or stationery
- Apply mood stamps

8.4.4 Terminal Server Edition and Citrix MetaFrame Overview

This section describes how the IBM Network Station, which is not an Intel-based processor, can run Windows NT desktop as well as other Windows applications. For example, an IBM Network Station user could run the Lotus Notes PC Client to access a Domino server on the AS/400.

Microsoft Windows NT Server 4.0, Terminal Server Edition (WTSE), formerly called Hydra, is an extension of the Windows NT Server network operating system product line that delivers the Windows operating system experience to diverse desktop hardware through terminal emulation.

What Windows Terminal Server provides is the same multi-user functionality that was provided by Citrix WinFrame, but at the Windows NT 4.0 level and an additional protocol to connect into the server. This protocol is called the Remote Desktop Protocol (RDP), and is the protocol used by Windows Terminals.

The IBM Network Station can use either the protocol called Independent Computing Architecture (ICA) or X11 to connect into WTSE. These protocols are not provided by WTSE.

The ICA functionality provided by Citrix's ICA protocol is still available but requires the installation of Citrix's MetaFrame product in addition to WTSE.

If the X11 functionality is also desired, then NCD's Unix Integration Services are required, in addition to MetaFrame.

Additional details on Citrix MetaFrame and NCD's UNIX Integration Service can be found respectively on the Web at: www.citrix.com and www.ncd.com

Note

This section does not cover Windows NT 4.0, Terminal Server Edition and Citrix MetaFrame Installation. For more detail about how to install this software, refer to *IBM Network Station Manager Release 3 Guide for Windows NT*, SG24-5221. This redbook can be found on the Web site: www.redbooks.ibm.com

8.4.5 Connecting IBM Network Station to Windows Terminal Server

The IBM Network Station supports either the ICA protocol, using a native ICA client running on the IBM Network Station (new with release 3 of the Network Station Manager) or the X11 protocol using the native X-server functionality as in previous releases. This section only describes connectivity to a Windows Terminal Server using ICA protocol that is provided by Citrix MetaFrame.

As mentioned previously, IBM Network Station now includes a local client called ICACLNT which uses ICA protocol to connect to a server running Terminal Server Edition and Citrix MetaFrame.

To setup the ICA client on your Network Station, sign on to the IBM Network Station Manager to access the Startup tasks. Then, define a local program Menu item as shown in Figure 148 on page 250.

Figure 148. Configuring an ICA Client

The client, *ICACLNT,* must be entered in the *Program to run* box. The term e *-host* is required in the *Parameter* i box. This is needed to indicate the target host. In our, example (Figure 148) we also used the term *-colors 16* to ensure no color blinking.

The syntax and usage of the `ICACLNT` client name is shown in the following example:

```
ICACLNT [-host hostname or ip address] [-options ...] [- - command args]
-help       <print out this message>
-ca[che]     <large cache size in KB>
-c[olor]     <16 | 256 color>
-g[eometry]   <Width x Height>
-ti[tle]     <Window name>
-na[me]      <client name>
```

8.4.6 Lotus Notes 4.6a Basic Installation on Windows Terminal Server

To access a Domino server from a Network Station using the Lotus Notes 4.6a client, the code must first be installed on the server.

The following procedure is intended to explain the basics of how to install Lotus Notes on Windows Terminal Server and probably need to be adapted according to the specific requirements of a given environment.

1. Log on as Administrator and map an *h:* (or whatever letter you want to use as the home drive for all your users) to the administrator's home directory.
2. Open a command prompt and enter the following command:

   ```
   CHANGE USER /INSTALL
   ```

3. Run the Lotus Notes 4.6 install program.
4. Check the **Install On a File Server** option on the very first window of the Notes Install. You are prompted for a **Name and Company** on this display.

5. Select the **File Server Install** option on the next Notes Install display.
6. The next display asks if you want to change the defaults option in the Typical vs. Custom Setup display. It is recommended that the **Custom Setup** option be chosen and that all features that are not needed are deselected. One very obvious feature is the *Notes Modem definitions*. The only options left selected are *Notes Workstation* and *Attachment viewer*.
7. Ensure that the destination directory is the server drive **c:** (or possibly **m:** if you remapped it).
8. Notes Installation copies all the files to your hard drive.
9. Click on **Done** when the Successful Installation message appears.
10. Run the Lotus Notes Node Installer by selecting **Start —> Programs —> Lotus Applications —> Node Installer**.
11. Do *not* put a person's name in the *Name* field because all users will get this setting. It is recommended that you put the company name in this field.
12. Specify **H:** drive as the P*ersonal Directory*. It is recommended that you leave the default directory. Therefore, you are installing to **h:\notes\data**.
13. The files are copied to the Administrator's *h:* drive. Click **Done** when successful installation has completed.

Attention

Do not launch Notes at this time.

14. Open **Windows Explorer**. Cut and paste **c:\wtsrv\notes.ini** to **h:\notes\data**
15. Copy the entire **h:\notes directory** to **c:\users\template**. This is done a in Windows Explorer by selecting the h:\notes directory.
    a. Right click on the **h:\notes** directory.
    b. Select **Copy.**
    c. Select the **c:\users\template** directory.
    d. Right click on the **c:\users\template** directory.
    e. Select **Paste**.

16. Create a text file called *nclogin.bat* in the *c:\wtsrv\system32\repl\import\scripts* directory that contains the same lines as this sample file *lotusnotesinstall.txt* shown in the following example. Be sure to replace *SERVERNAME* with your server's name.

```
REM This section is to determine if the user home directory exists
REM and create one if it does not
net use x: /d
net use x: \\SERVERNAME\users
if not exist x:\%username% md x:\%username%
net use x: /d
REM This part is for mapping the user home directory to H:
subst h: /d
subst h: \\SERVERNAME\users\%username%
REM This section is for setup of Lotus Notes client
if not exist h:\notes md h:\notes
if not exists h:\notes\data md h:\notes\data
if not exists h:\notes\data\notes.ini
copy c:\users\template\notes\data\*.* h:\notes\data
```

17. Use the following steps to assign the login script to all users in *User Manager for Domains:*

    a. Select **Start —> Programs —> Administrative Tools — > User Manager for Domains**.

    b. While holding down the **Ctrl** key, click on *all t*he users who will be using Notes.

    c. After all desired users are selected, click on **User —> Properties**.

    d. Select **Profile** and enter **nclogin.bat** in the *login Script* field.

18. Use the following steps to create a common icon for all users to run Lotus Notes:

    a. Right click on the **Start** button.

    b. Select **Explore All Users**.

    c. Select **Profiles —> All Users —> Desktop** click on **File —> New —> Shortcut**.

    d. Enter **c:\notes\notes.exe** from the command line and click **Next**.

    e. Enter *Lotus Notes* for the description and click on **Finish.**

19. From the *Windows Explorer*, right click on the newly created Lotus Notes Shortcut. Select **Properties**. Go to the **Shortcut** tab. Change the *Start In* field to be **h:\notes\data**.

20. Go to the command prompt and enter the following command:

```
CHANGE USER /EXECUTE
```

When a user logs on the next time, their user directory is automatically created, mapped to *h:*\, and the Lotus Notes Workstation set up as an application as shown in Figure 149.

Figure 149. Lotus Notes Workstation on IBM Network Station

Appendix A. Flash Card Scenarios

This appendix contains examples of the *flash.nsm* and *peer.nsm files* and a list of the files and directory structure that must be loaded onto the Flash card for the relevant application support.

In all cases the source directory structure is */QIBM/ProdData/NetworkStation.* For example, the file ACTLogin is sourced from */QIBM/ProdData/NetworkStation/mods/* and must be placed in the directory /local/mods/ on the Flash card. The path /local/ is the root directory of the Flash card.

In each of the following examples, the kernels are listed. You must decide on which kernel to use depending on the available space on the Flash card file system.

A.1 Support for 5250, 3270, and VTxxx Emulation

The following files must be copied to the Flash card to support the start-up of the IBM Network Station and to run the 5250, 3270 and VTxxx support from the Flash Card.

The number of bytes used for this scenario is 5,608,358 if the compressed kernel for the series 100 and 300 is used.

The path */local* is the root of the Flash Card file system.

/local/boot.nsl

kernel[kernel.Z, kernel.63a, kernel.63Z]

/local/mods/

actlogin.nws
colormap.nws
export.nws
filed.nws
libconf.nws
libmlc.nws
libprapi.nws
libprxapi.nws
lpd.nws
lprd.nws
mcuis.nws

© Copyright IBM Corp. 1999

miscpr32.nws
mwm.nws
nfsd.nws
ns3270.nws
ns5250.nws
ns5250xx.nws
nsterm.nws
sbcs_im.nws
seriald.nws
term.nws

The *flash.nsm* file and *peer.nsm* files are also shown as an example. Please note that the *flash.nsm* file contains lines that are optional depending on whether you intend to use the peer boot functionality.

Flash.nsm File Example

```
# flash.nsm - This file resides in the /QIBM/ProdData/NetworkStation/configs directory
#
# AS/400 File Service Table
#
set file-service-table = {
{"/netstation/prodbase" nil 10.1.1.30 tftp "/QIBM/ProdData/NetworkStation/" unix 3 30 4096 4096 }
{"/QIBM/ProdData" nil 10.1.1.30 tftp "/QIBM/ProdData/" unix 3 30 4096 4096 }
}

# Read the configuration files from the server
#
read standard.nsm
#
# Make the necessary mods to the base values
#
set boot-desired-source = local
set boot-second-source = none
set boot-third-source = none
set exec-startup-commands = {
{ mcuis }
{ "actlogin -authserv <servIPaddr>" }
}
# Where <servIPaddr> is the AS/400 system IP address, the authentication server.

# The next line enables the NFS server Daemon for peer boot and is required if the flash card file
#system is to be mounted to the AS/400 IFS.

set file-enable-nfs-server = true
#
#The next two lines are required for peer boot only.
set file-export-directory-list = { { "/peerboot" "/local" } }
set file-nfs-access-control-default = read-only
#
# The next 4 lines are optional and enable the local file manager which can be accessed using
# TELNET or from the console window on the Network Station.
set xserver-initial-x-resources = "ncdconsole.disable.TerminalMenu: false"
set file-manager-password = nws1red
set file-manager-access-control-enabled = true

set file-try-all-matches-on-open = true
# Set up to get executable modules from the flash card
set modules-directory = /local/mods
```

Peer.nsm File Example

```
#
# peer.nsm - place onto the flash card in /local/configs and into
# /QIBM/ProdData/NetworkStation/configs
#
#Set up the file service table to access the server
set file-service-table = {
{"/netstation/prodbase/configs/" nil 10.1.1.2 tftp "/QIBM/ProdData/NetworkStation/configs/" unix 3 30 4096
4096 }
{ "/QIBM/ProdData/NetworkStation/configs/" nil 10.1.1.2 tftp "/QIBM/ProdData/NetworkStation/configs/" unix
3 30 4096 4096 }
{ "/netstation/prodbase/" nil 10.1.1.2 tftp "/QIBM/ProdData/NetworkStation/" unix 3 120 4096 4096 }
{ "/QIBM/ProdData/" nil 10.1.1.2 tftp "/QIBM/ProdData/" unix 3 30 4096 4096 }
}

# Read the base configuration files on the server.
read standard.nsm
#
# Make the necessary mods to the base values
set boot-desired-source = nfs
set boot-nfs-directory = /peerboot/
set boot-second-source = none
set boot-third-source = none
set exec-startup-commands = {
{mcuis }
{ "actlogin -authserv <serverIPaddr>" }
}
# Where <servIPaddr> is the AS/400 system IP address, the authentication server.
set file-try-all-matches-on-open = true
#
# Set up to get Java modules, if any from the flash card
# set java-directory = /peerboot/java
#
# Setup to get executable modules from the flash card
set modules-directory = /peerboot/mods
```

A.2 Support for 5250, 3270, and VTxxx with Fonts

Network traffic can be reduced by adding the font files required for the application to the Flash card. It is difficult, and is often a case of trial and error, to ensure all of the necessary fonts required by the application are located on the Flash card.

Attention

Please be aware that when the fonts directories are stripped down, the *fonts.dir* file (this file contains a directory of available fonts) must be updated to reflect that not all of the original fonts are located on the Flash card. The utility required to do this, *mkfontdir*, is generally only available on UNIX systems. This limits your ability to scale down the font directories unless you have access to a UNIX system.

This section was added for your reference.

If the uncompressed kernel for the Series 100 and 300 Network Stations is used, the number of bytes required is 7,966,842 bytes.

There are over 25MB of font files and these also vary by locale. However, we recommend that font information is loaded from the server.

/local/

KeysymDB
boot.nsl
kernel [kernel.Z,kernel.63,kernel.63Z]
rgb.txt

/local/SysDef/

ibmwall.xbm
inetvars.nsm
nsminv.txt
startup.nsm
tiles.xbm

/local/SysDef/NCDwm/

pref

/local/SysDef/NS3270/

pref

/local/SysDef/NS5250/

pref

/local/X11/app-defaults/

mcuis
Mwm
system.mwmrc

/local/X11/fonts/pcf/i18n/

Block11.iso1_UCS.pcf.Z
Block17.iso1.UCS.pcf.Z
Ergo15.iso1_UCS.pcf.Z
Ergo17.iso1_UCS.pcf.Z
fonts.dir

/local/X11/locale/

locale.alias
locale.dir

/local/X11/locale/UTF-8_BASE-0/XLC_LOCALE

/local/X11/locale/UTF-8_C/XLC_LOCALE

/local/X11/locale/UTF-8_iso8859-1/XLC_LOCALE

/local/mods/

actlogin.nws
colormap.nws
export.63a
export.nws
filed.nws
libconf.nws
libmlc.nws
libprapi.nws
libprxapi.nws
lpd.nws
lprd.nws
mcuis.nws
miscpr32.nws
mwm.nws
nfsd.nws
ns3270.nws
ns5250.nws
ns5250xx.nws
nsterm.nws
sbcs_im.nws

seriald.nws
term.nws

A.2.1 The Flash.nsm File Additions to Support Local Font Storage

To support local font storage, the following lines must be added to your *flash.nsm* file.

Flash.nsm File Additions

```
# Add these lines to flash.nsm
#
# Get the background screen and screensaver from the flash card filesystem

set pref-screen-background-bitmap-file = "/local/SysDef/ibmwall.xbm"
set pref-screensaver-bitmap-file = "/local/SysDef/ibmwall.xbm"
set xserver-keysym-file = /local/XKeysymDB
set xserver-rgb-file = /local/rgb.txt
set xserver-default-font-path = {
        {"/local/X11/fonts/pcf/i18n"}
        {"built-ins"}
}
```

A.2.2 The Peer.nsm File Additions to Support Local Font Storage

To support local font storage, the following lines are required in your *peer.nsm* file.

Peer.nsm File Additions

```
# Add these lines to peer.nsm
#
# Get the background screen and screensaver from the flash card file system.

set pref-screen-background-bitmap-file = "/peerboot/SysDef/ibmwall.xbm"
set pref-screensaver-bitmap-file = "/peerboot/SysDef/ibmwall.xbm"
set xserver-keysym-file = /peerboot/XKeysymDB
set xserver-rgb-file = /peerboot/rgb.txt
set xserver-default-font-path = {
        {"/peerboot/X11/fonts/pcf/i18n"}
        {"built-ins"}
}
```

A.3 Support for NC Navigator with Java Virtual Machine

The files required to start the Network Station and run the NC Navigator Browser and the Java Virtual Machine from the Flash card is found in this section.

There is no change to the *flash.nsm* and *peer.nsm* files because all of the configuration for NC Navigator is done on the server using IBM Network Station Manager program. The only difference is the files which are required on the Flash card. This setup requires at least 20 megabytes of storage space on the Flash card, if the uncompressed kernels for all systems are used.

If the compressed kernel and mods files for only the Series 100/300 or Series 1000 is required, the size drops to less than 16 Mbytes.

For more information about configuring and using NC Navigator for the Network Station, refer to the manual *IBM Network Station Manager Installation and Use,* SC41-0664.

Disk caching should *not* be used when running NC Navigator with Flash card support. The system is shipped with disk caching disabled, and this setting should *not* be changed because of the limitation of the Flash card. Refer to Chapter 3, “Using Flash Cards with the Network Station” on page 63 for more information.

The byte count for the files listed here, with support for the Series 100,300 and 1000 using uncompressed kernels, is 21,333,568 bytes.

The following is a list of the files required on the Flash card:

/local/

boot.nsl
kernel [kernel.Z, kernel.63a, kernel.63Z]

/local/java/

classes.zip
javacpa0.gif
javacpat.gif
nwshacl.zip
nwspackg.zip

/local/java/lib/

appletviewer.properties
awt.properties
content-types.properties
font.properties
font.properties.en
javac.properties
rmic.properties
serialver.properties

/local/java/lib/security/

java.security

/local/mods/

actlogin.nws
desktop.nws
export.63a
export.nws
filed.nws
java.63a
java.nws
jawt.63a
jawt.nws
jcomm.nws
jjpeg.63a
jjpeg.nws
jmath.63a
jmath.nws
jmmedia.63a
jmmedia.nws
jnet.63a
jnet.nws
jsysresource.nws
jzip.63a
jzip.nws
libconf.nws
libmlc.nws
libprapi.nws
libprxapi.nws
loaddb.nws
lpd.nws

lprd.nws
mcuis.nws
miscpref.nws
mwm.nws
navio.nws
nfsd.nws
sbcs_im.nws
seriald.nws

A.4 Support for ICA Client

In this scenario, the Network Station is started and the ICA client is loaded from the Flash card. The ICA client enables the Network Station to connect to a multi-user NT server running WinCenter or Citrix MetaFrame.

There is no change required to the *flash.nsm* and *peer.nsm* files. This setup requires at least 10 megabytes of free space on the Flash card if the uncompressed kernels for all systems are used.

If the compressed kernel and executable modules for only the Series 100/300 or Series 1000 are required, the size drops to less than 6 megabytes.

The following files are required to support ICA when booting from a Flash card:

/local/

boot.nsl
kernel [kernel.63a, kernel.Z, kernel.63Z]

/local/mods/

actlogin.nws
export.63a
export.nws
filed.nws
icaclnt.nws
icaui.nws
libconf.nws
libmlc.nws
libprapi.nws
libprxapi.nws
lpd.nws
lprd.nws
mcuis.nws

nfsd.nws
sbcs_im.nws
seriald.nws

A.5 Java Application Support

In this example, the Network Station is started from the Flash card with the intent to run a Java application from the Flash card. Using compressed kernels requires approximately 16 megabytes of space on the Flash card plus the java application you want to run.

This example has not been tested. The list is intended as a starting point to identify which files are required by the Network Station to support a Java application. Some modification to this list maybe required to support your java application.

/local/

boot.nsl
kernel [kernel.63a, kernel.Z, kernel.63Z]

/local/java/

classes.zip
javacpa0.gif
javacpat.gif
nwshacl.zip
nwspackg.zip

/local/java/lib/

appletviewer.properties
awt.properties
content-types.properties
font.properties
font.properties.en
javac.properties
rmic.properties
serialver.properties

/local/java/lib/security/

java.security

/local/mods/

actlogin.nws

export.63a
export.nws
filed.nws
java.63a
java.nws
jawt.63a
jawt.nws
jcomm.nws
jjitc.63a
jjpeg.63a
jjpeg.nws
jmath.63a
jmath.nws
jmmedia.63a
jmmedia.nws
jnet.63a
jnet.nws
jsysresource.nws
jzip.63a
jzip.nws
libconf.nws
libmlc.nws
libprapi.nws
libprxapi.nws
libprdbcs.nws
mcuis.nws
mwm.nws
nfsd.nws
sbcs_im.nws
seriald.nws
setup.nws

Appendix B. Executable Module Descriptions

The appendix attempts to outline each module, found in release 3.0, with a brief description of the modules function. This is not a definitive listing. However, it provides some information on what each module is used for.

B.1 Module Information

Table 20. Module Information

Module Name	Module file ID	Type	Description
ACTLogin	actlogin.nws	client	Login Authentication Manager
audio	audio.nws	extension	Network Audio
color map	colormap.nws	extension	3270/5250 color map
desktop	desktop.nws	extension	Used by NC Navigator
export	export.nws export63a.nws	library	Symbols exported by the kernel
filed	filed.nws	daemon	Local file manager daemon
help	helpview.nws	extension	Help Viewer
Java Agent	jagent.nws	extension	Domino Support
Java	java.nws	extension	Java Virtual Machine
Java Abstract Window Support	jawt.nws	extension	Java Windowing Package
Java JPEG	jjpeg.nws	extension	Java JPEG
Java Math	jmath.nws	extension	Java Mathematical Formulas
Java MultiMedia	jmmedia.nws	extension	Java Multi Media
Java Networking	jnet.nws	extension	Java Networking
Java NWS Browser	jnsb.nws	extension	Java Network Station Browser

Module Name	Module file ID	Type	Description
Java system information	jsysresource.nws	extension	Java System Resource Info.
Java Zip	jzip.nws	extension	Uncompress Java ZIP files
keymap52	keymap52.nws	extension	5250 Keyboard map editor local client.
libconf	libconf.nws	library	Configuration Library
libmlc	libmlc.nws	library	Used by Console => Setup
libppp	libppp.nws	library	PPP Protocol library
libprapi	libprapi.nws	library	AIX printer library
libprxapi	libprxapi.nws	library	X Windows library
loadb	loadb.nws	utility	module loader (NC Navigator)
login	login.nws	utility	login local client
Mini-Console	mcuis.nws	utility	Provides a pop up error console
miscpref	miscpref.nws	utility	5250 Miscellaneous Preference
Motif Window Manager	mwm.nws	client	Window manager
NC Navigator	nav128.nws	Client	NC Navigator 128 bit (US Only)
NC Navigator	navio.nws	client	NC Navigator browser 40 bit.
NFS Daemon	nfsd.nws	daemon	Network File System Daemon
Terminal Emulation	nsterm.nws	client	VTxxx Emulator
NS3270	ns3270.nws	client	3270 Emulator
NS5250	ns5250.nws	client	5250 Emulator

Module Name	Module file ID	Type	Description
pref	pref.nws	utility	Change user preferences (from the console)
qsetup	qsetup.nws	utility	Change Quick Setup (from the console)
Serial Daemon	seriald.nws	extension	Serial/Parallel port daemon
Setup	setup.nws	utility	Change setup parameters (from the console)
show	show.nws	utility	Show Memory usage (from the console)
SIE	sie.nws	extension	SImple Image Extension (not used)
Statistics	stats.nws	utility	Show system statistics (from the console)
Terminal Emulator	term.nws	client	VTxxx Emulator
Touch display	touchscr.nws	client	Touch Screen Support
Network test	test.nws	utility	Test Network (from the console)
Window Manager	wm.nws	client	Built in Window manager
Xinput	xinput.nws	client	Required for Touch Screen calibration

Appendix C. 5500 Express IP Control Unit

This appendix, which presents an overview of the IBM 5500 Express IP control unit, includes some technical details and example configurations. This product was not available at the time of writing. However, we provide this information to give you a more complete view of WAN connection capabilities.

C.1 5500 Express IP Control Unit

The 5500 Express IP Control Unit allows you to connect Network Stations or personal computers equipped with an IBM Express Twinax Adapter to a remote AS/400 system. The unit establishes these connections using TCP/IP. The 5500 manages traffic between clients and the AS/400 system.

Although the clients physically connect to the twinax cable, these connections appear to as a LAN connection to the client IP applications.

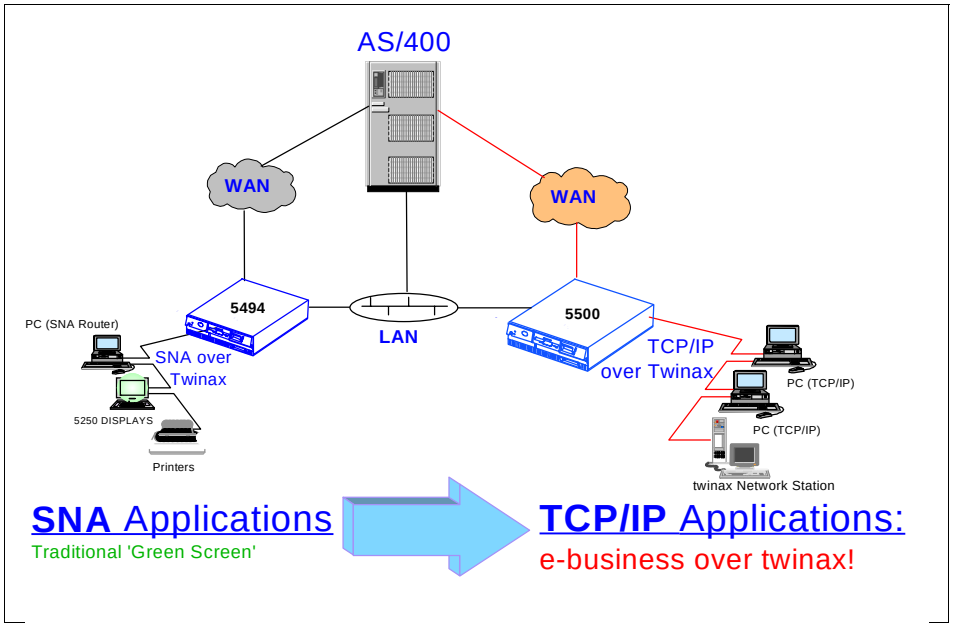


Figure 150. Transition from SNA to TPC/IP with 5500 Control Unit

In Figure 150, you can see the simplicity of transition and coexistence with an existing SNA network.

© Copyright IBM Corp. 1999

The 5500 control unit provides connection to:

- Express twinax clients attached to AS/400 systems running V4R1 or earlier. This connection is established either though LAN or WAN and SLIP.
- For AS/400 systems running V4R2 or later release, the connection is still through LAN or WAN, but the PPP and SLIP are available.

The 5500 supports the latest IP/Twinax devices. IBM 5250 Express Adapters and IBM 5250 Adapters (ISA) PCs with IBM 5250 adapters require no new hardware Twinax Network Stations (8361-341). However, the 5500 Controller does not currently support PC's using SNA, NPT's or printers

This new controller provides new capabilities for twinax attached PCs. These PCs can run Web Browsers, Lotus Notes or Domino, file or printer sharing, and so on.

You now have compatibility with Client Access/400 and Personal Communications AS/400 (by changing protocol from SNA to TCP/IP)

The 5500 uses the 5250 Express support to increase throughput by four times over legacy twinax. There is also support for enhanced cable lengths:

Twinax: 1.2Km (4K ft.) @ 2Mbps, 1.4Km (5K ft.) @ 1Mbps

UTP: .96Km (3.2K ft.) @ 2Mbps, 1.3Km (4.2K ft.) @ 1Mbps (w/IBM 7299)

UTP+Fiber: 3.2Km (10.7K ft.) @ 2Mbps, 3.7Km (12K ft.) @ 1Mbps (w/IBM 7299)

C.1.1 Twinax Client Connection Requirements

The following list of requirements allow connection of the 5500 Express IP control unit to the client workstation:

- PC workstations with a minimum 486 processor and PCI (Peripheral Component Interconnect), PCMCIA (Personal Computer Memory Card International Association), or ISA (industry standard architecture) slots.
  - IBM 5250 Express Adapter or 5250 Enhanced Emulation Adapter as listed below 1.
  - Twinax cabling to 5500 Control Unit control unit eight-port breakout box.

    Note: Cables are not included in the 5500 control unit package.
  - IBM 5250 Express TCP/IP Driver 1.27 or higher. To obtain the latest copy of the driver, see the website:http://www.networking.ibm.com

– One of the following operating systems:
  - MS Windows NT 4.x with Service Pack 3
  - MS Windows 95 with Service Pack 1
  - MS Windows 98

- Twinax IBM Network Station 8361-341 with 24 megabytes RAM minimum memory and Network Station Manager program Release 3.0 or higher.

Note

The 5500 Control Unit is not a router or a DHCP relay agent. Therefore, 5500 twinax clients cannot make DHCP requests unless there is a DHCP server on the twinax segment, or a DHCP Server on a 5500 LAN segment and the twinax subnet is configured as part of that LAN. Clients on the second 5500 LAN segment cannot communicate with the DHCP server on the first LAN. For DHCP requests to travel across a WAN, a LAN-based router must be installed with a relay agent.

C.2 Connection Configurations of the 5500 Control Unit

The IBM 5500 Express IP controller can be part of your network in a number of different configurations. Five typical network layouts are shown in this section.

Although typical applications of the 5500 control unit, these examples are just a few of the many ways you can exploit the unique features and characteristics of this controller.

IBM recommends that, when using the 2Mbps Mode, install your Express devices on a different port than your legacy devices. Also, ensure that you have Express-enabled hubs and multiplexers (IBM 7299). IBM 5500 in an Express environment.

Figure 151 shows an example of an IBM 5500 used in a 5250 Express environment with a fiber optic link to a multiplexer.

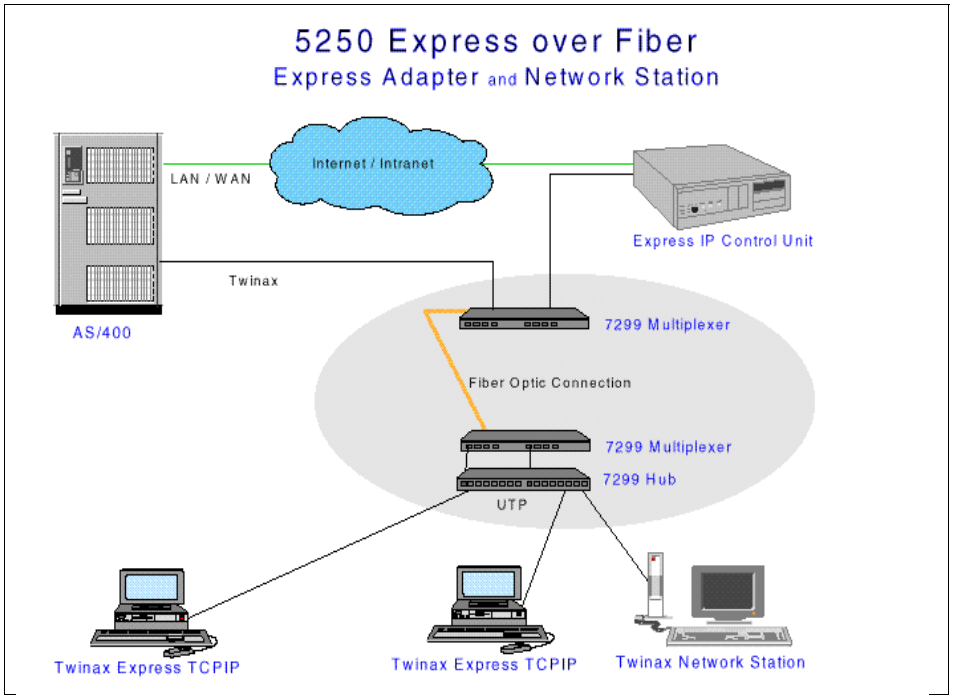


Figure 151. IBM 5500 in an Express Environment

Figure 152 shows an example of an IBM 5500 in a complex combination of network media types.

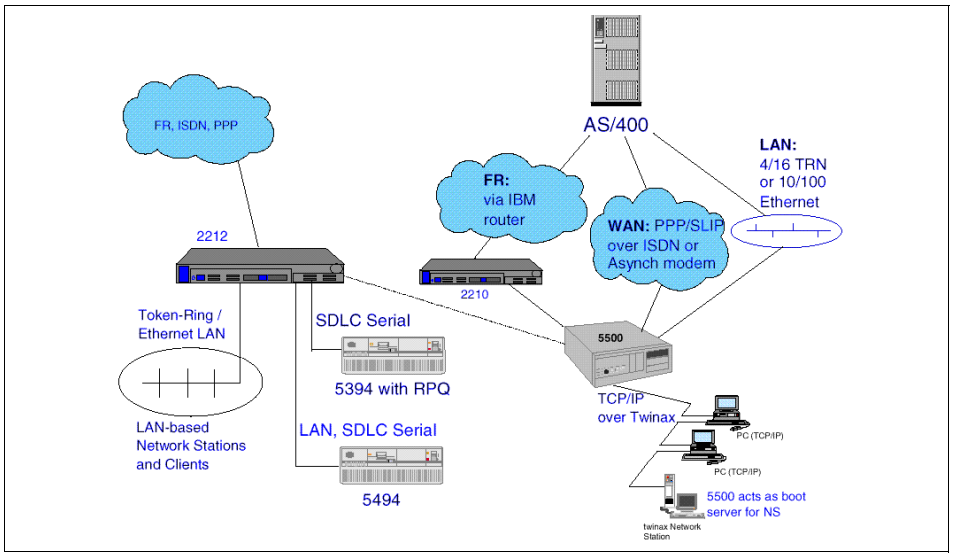


Figure 152. IBM 5500 with a Combination of Media Types

Figure 153 shows an example of the synchronous modem for the WAN connection between an AS/400 system and IBM 5500.

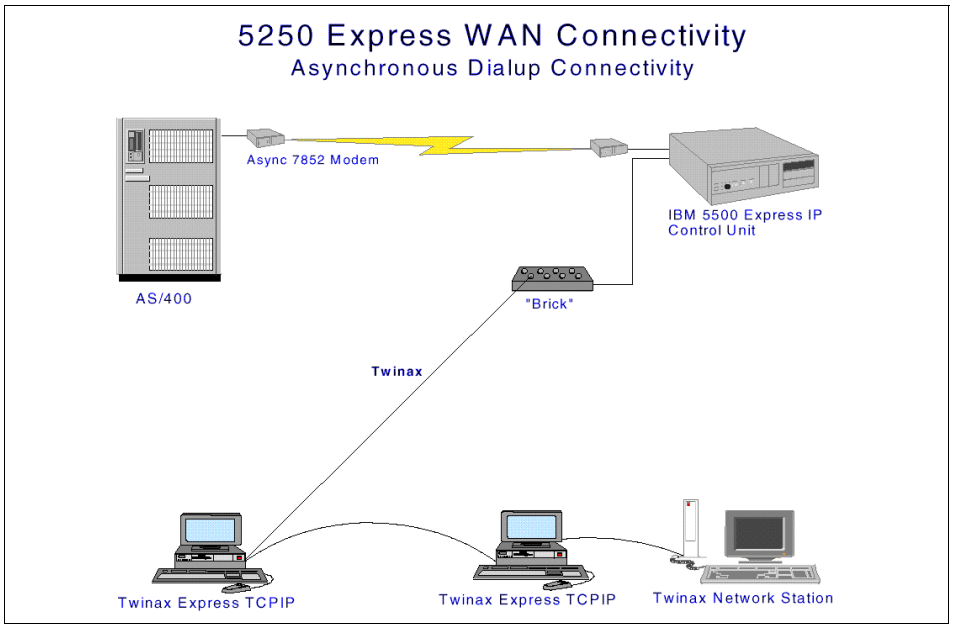


Figure 153. Asynchronous Dialup Connectivity

Figure 154 shows an example of a frame relay WAN connection to the IBM 5500 providing connectivity for remote terminals.

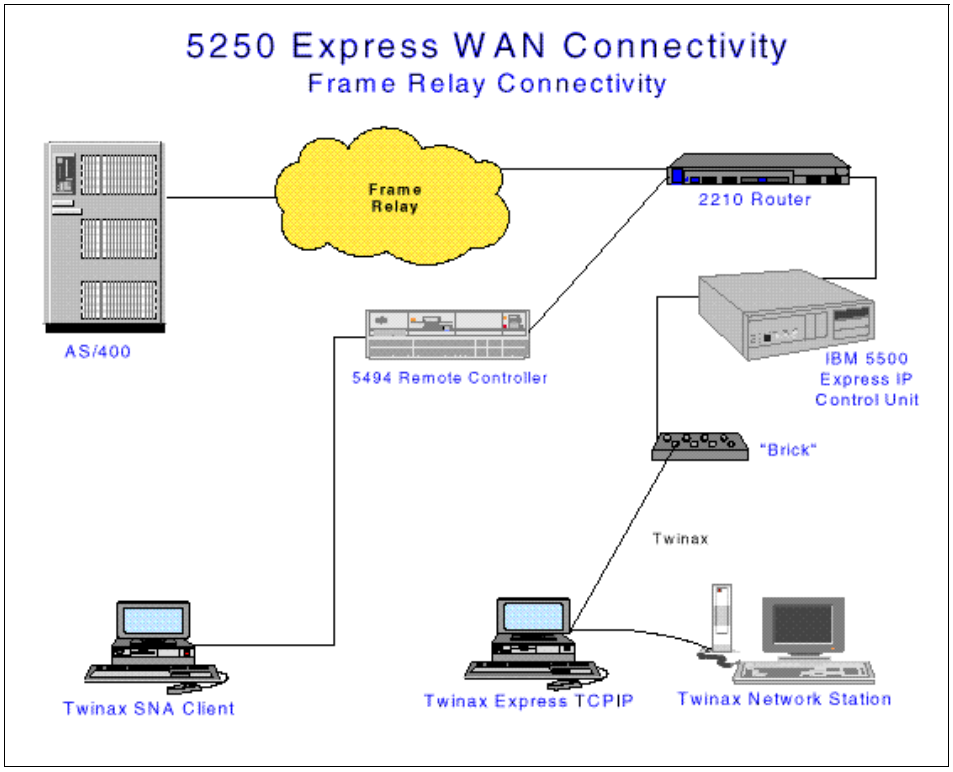


Figure 154. Frame Relay Connectivity

C.2.1 WAN Configuration Data

To successfully configure the WAN connection for the 5500 control unit to the host (AS/400 system), the following information is necessary:

- Valid Phone Number and Baud Rate

  A valid baud rate must have one of the following values:

110	300	1200	2400	4800
9600	19200	38400	57600	115200

C.2.1.1 Understanding IP Address Requirements

Obtaining contiguous IP addresses may be difficult. Be prepared by obtaining extra addresses for future use.

Valid Internet protocol (IP) addresses must meet the following criteria:

- Four decimal numbers separated by periods.
- Number one must be greater than or equal to 1 and less than or equal to 223.
- Numbers two, three, and four must be greater than or equal to zero (0) and less than or equal to 255.
- All IP addresses must be unique.
- The IP Address must not equal the Net Address
- IP Address must not equal the Broadcast Address

C.2.2 ISDN Modems

If you use an ISDN modem with your 5500 control unit for dial-up WAN connectivity, additional configuration is necessary. Parameters, such as Switch Type, Service Profile IDs (SPIDs), Directory Numbers (DNs), Terminal End-point Identifiers (TEIs), and Call Type, must be entered and saved on your ISDN modem. Typically, these fields can be configured using the AT command set or software provided with your ISDN modem. Because these parameters must be set prior to connecting the modem to the 5500 control unit, IBM recommends that you use a personal computer (PC) or other RS-232 capable device to configure these parameters. Attach the ISDN modem the 5500 control unit.

Consult the documentation provided with your ISDN modem for more details on the parameters required by your modem and the steps necessary to configure them.

C.3 5500 Control Unit and TCP/IP LAN Concepts

The most common configurations for the IBM 5500 Express IP control unit are:

- The AS/400 system is connected through the WAN interface with the LAN connected using Ethernet or token-ring interface. Workstations on LAN are twinax-attached workstations (either Network Stations or PCs with 5250 Express emulation adapters).

- The AS/400 system is connected through the WAN interface of the 2210 router. LAN is connected to the 2210 router and existing 5494 with twinax workstations initially connected to the 5494 migrating to the IBM 5500 control unit.

C.3.0.1 Gateways and IP Addresses

As part of planning the installation of your 5500 control unit, determine the range of addresses to be used by each network port of the 5500 control unit. The twinax port allows up to 56 twinax-attached workstations to exploit the TCP/IP protocol for access to network resources.

C.3.0.2 Subnetting

The 5500 control unit is unique because it allows you to use the subnetting of an address space to define the addresses that can be used for the twinax workstations without making subnet mask or default router changes to existing LAN workstation or router configurations.

The 5500 control unit forwards IP packets, allowing all devices attached to the 5500 control unit to communicate with each other. It is not necessary to configure a default router for devices attached to the 5500 control unit. Any TCP request that is sent to an IP address in the network associated with any port of the 5500 control unit is routed to that port. The 5500 control unit implements an extended ARP (Address Resolution Protocol) agent to send packets to twinax-attached TCP/IP workstations based on the twinax port using a subnet of the network assigned to the LAN port 0 of the 5500 control unit . If the destination IP address is outside the range of addresses known to the 5500 control unit (or any default gateways configured for the workstation), then the request fails.

If a LAN-attached device performs the function of a router to the Internet, the IP address of that device should be used as the default gateway for that network segment. This action grants Internet access to all workstations attached to the 5500 control unit provided the address space used by those workstations is properly coordinated so that your domain is known to the Internic domain name server.

C.3.1 Installing the IBM 5500 into an Existing Network

One of the most common applications of the IBM 5500 control unit is to allow existing twinax workstations that are remotely connected to an AS/400 system through a 5494 control unit, to be properly migrated to the IBM 5500 control unit. This application expands their use to the new e-business applications. Under this circumstance, or for any other application where the IBM 5500 Unit is placed on an existing LAN, you must decide whether to

subnet the IBM 5500 control unit or to obtain an additional set of addresses for the twinax workstations attached to the control unit. Should you decide to obtain a new address space, the routing tables in routers that are upstream from the IBM 5500 control unit must be manually updated to include the new address space. You would have to coordinate those addresses with the Internic (if Internet access is desired) and default router addresses to be configured in the twinax workstations, which are more complex to determine. Manual table updates are required because the IBM 5500 control unit does not run any routing protocols (RIP, RSPF, and so on). IBM recommends that, when you install the 5500 control unit into an existing network, you should subnet your existing address space to avoid problems.

C.3.1.1 Subnetting Example

Subnetting is accomplished by partitioning an existing address space and using each set of addresses for different sets of devices. Partitioning is accomplished by using a subnet mask that is more restrictive for the twinax workstations attached to the 5500 control unit than for the LAN to which the 5500 control unit is also attached. The following is a simple example:

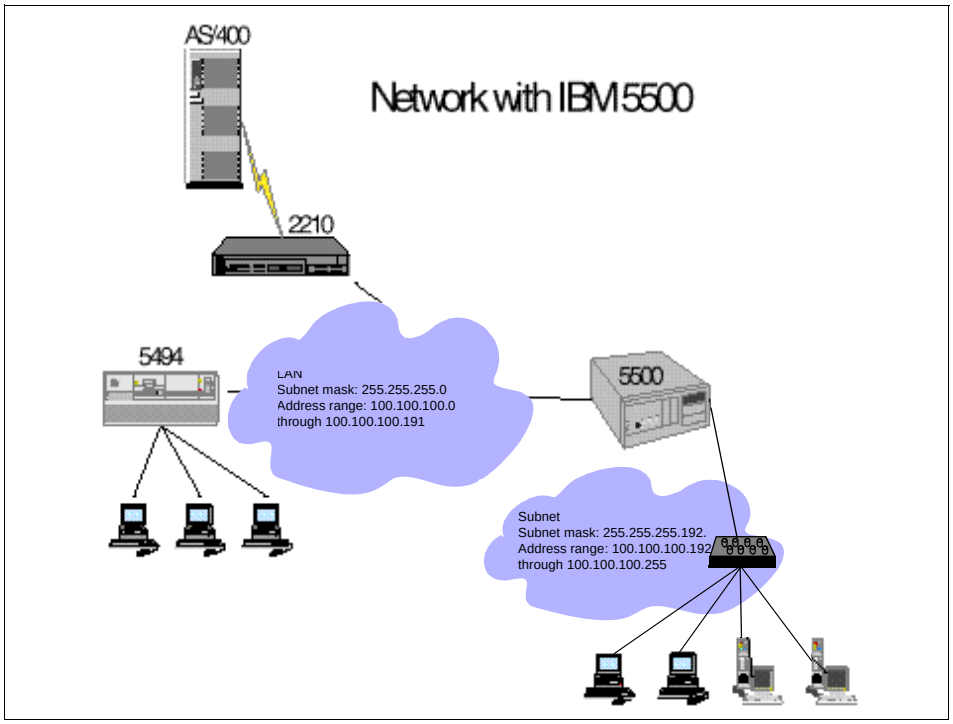


Figure 155. 5500 Subnet Example

- Original network uses subnet mask 255.255.255.0 and is assigned addresses 100.100.100.0 through 100.100.100.255 (See Figure 155)
- Desire to split this address space so that 64 addresses are reserved for use by the twinax workstations attached to the IBM 5500 control unit and 192 addresses are left for other LAN devices.
- Twinax workstation use subnet mask 255.255.255.192 and can take any contiguous 64 addresses between 100.100.100.0 and 100.100.100.255. We is highly recommended that the twinax workstations use the upper end of the available range of addresses, in this case 100.100.100.192 through 100.100.100.255. It is also critically important that none of the addresses in the range reserved for the twinax workstations be assigned to any device anywhere else on the network.
- Because three of these addresses are consumed by the TCP/IP network architecture (you should not use the first, second or last address in the range), there are 61 addresses left for use by twinax workstations attached to the IBM 5500 control unit.(100.100.100.194 through 100.100.100.254).
- No upstream router table changes are required because the IBM 5500 control unit and the total address space is already properly routed to the existing LAN.

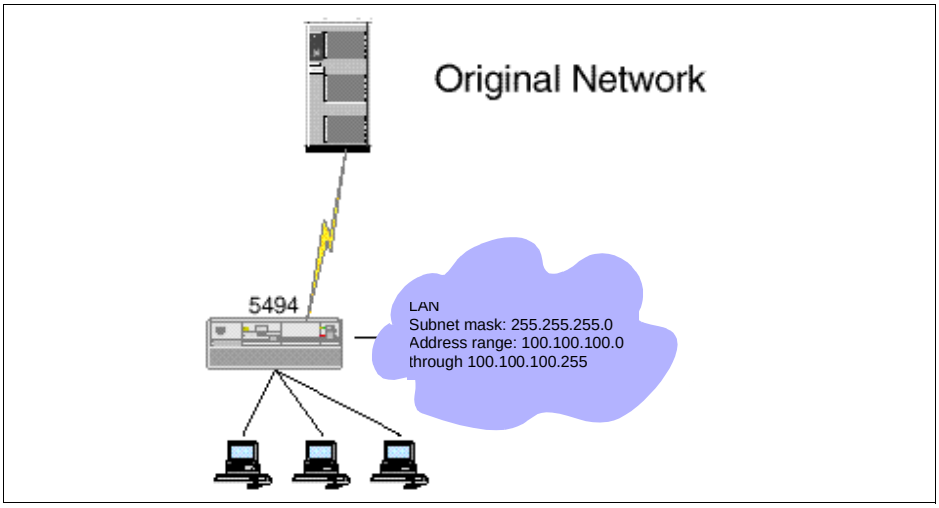


Figure 156. Example of a Network before Installing the IBM 5500

- No subnet mask changes are required on devices attached to the LAN (any other time you subnet a network all of the subnet masks must be changed to reflect the network number for each subnet). You must assign

a different address to any device on the LAN that is using one of the addresses in the range of addresses subnetted to the twinax workstations.

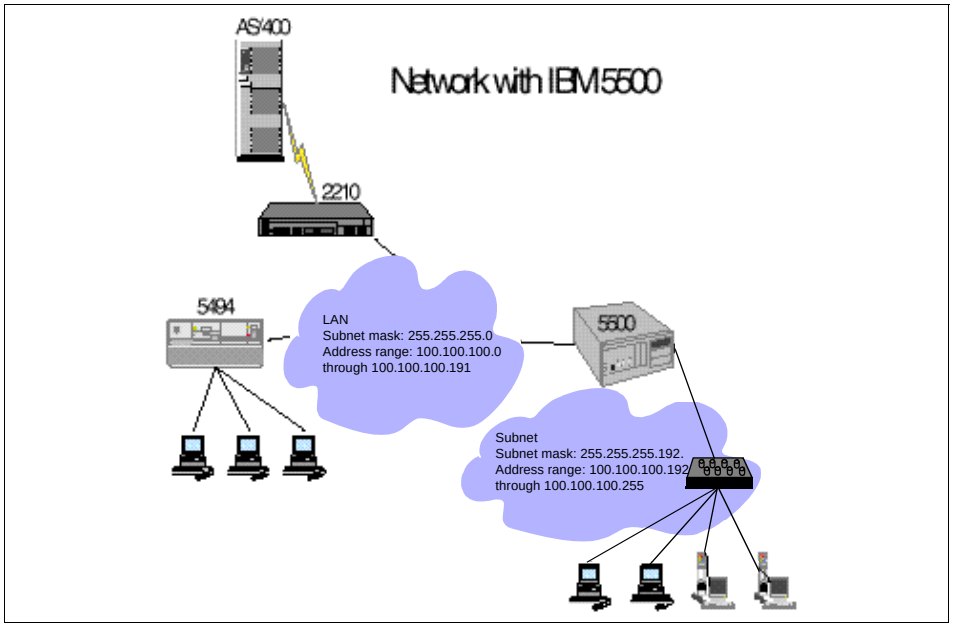


Figure 157. Example of a Network after Installing the IBM 5500

C.4 Optimizing Twinax Performance for the Client Workstation

To maximize your twinax performance for the client workstation, follow these recommendations when using the configuration program:

IP Broadcasting Setting

Use the *Local* or *None* setting. The Local setting allows the devices on the twinax subnet to recognize each other. The IP Broadcasting Transparent (or default) setting allows non-twinax devices to include the twinax subnet in the *Network Neighborhood*, and the twinax devices subnet to include the non-twinax subnet in the *Network Neighborhood*. However, this function can degrade twinax performance if the 5500 control unit is attached to a large network.

Dual Mode Setting

Every twinax workstation controller (WSC) handles ports one at a time. Every device must wait until the WSC can handle its port. An older WSC has eight

ports to time slice. However, the 5500 control unit's WSC is actually two mini-controllers, each responsible for servicing 4 ports.

Setting the 5500 control unit's dual mode operation to *Enable* allows each device to obtain quicker service. To maximize performance, balance the load between the two mini-controllers, dividing your devices equally between ports 0 through 3 and ports 4 through 7.

Using Twinax Multiplexers

The use of twinax multiplexers can prevent and increase in performance. Multiplexers combine the signals of multiple ports into a single cable for a longer transmission run. The signals are de-multiplexed into separate ports. Older multiplexers, such as the IBM 6299, were developed before the invention of a dual mode WSC. For an older multiplexer to combine all eight ports of a dual mode WSC, the two mini-controllers must be reconfigured to function as a single controller. This can result in a loss of performance. Setting the 5500 control unit's dual mode operation to *Disable* reproduces this action and can reduce performance.

Instead of decreasing performance, we recommend that you use a new multiplexer, the IBM 7299. This multiplexer uses time domain multiplexing to combine the signals from the two active mini-controllers.

5250 Express Data Stream

The independent modes available on the 5250 Express data stream is the *Optimized Mode*. It offers point-to-point communications with an Express device. This mode is ignored by other devices and works in any valid cabling configuration.

C.5 Using the 5500 Control Unit as a Network Station Boot Server

The 5500 control unit makes a good alternative boot server. This help reduce network traffic and improves local bootup times. This control unit can be used at any remote site that does not have a local server. It serves the remote NPT customers as a great way to improve the function delivered to their remote sites, allowing twinax NPTs to move to twinax Network Stations without the need to change cabling.

Using the 5500 control unit as a boot server for IBM Network Stations requires that you perform NVRAM setup on your Twinax Network Station. When used in this mode, the NSM (Network Station Manager) configuration server builds a text file called *defaults.dft*. This file is built in the configuration directory of the client's NSM configuration server, for example: *instation*\ *prodbase**configs.*

This file also prevents the NSM configuration server from changing the NVRAM settings. The 5500 control unit uses TFTP protocol to transfer the operating system kernel files but changes to NFS by default.

The NC user should avoid selecting the ROAM function. By default, the authentication login display points to the TCP/IP address of the 5500 control unit (when using the 5500 control unit to boot from). The user is forced to click on the ROAM button and enter the TCP/IP address of the NSM configuration server.

To prevent these actions, add the following information to the *nstation**prodbase**configs*\ directory.

Table 21. The Defaults.dft File

set config-auto-save-nvram **= false**	Causes the NC not to update its NVRAM
set exec-startup-commands = **{{"actlogin -authserve TCPI-PADDR"}}**	Allows the NSM Admin to boot server and have login display on Configuration NSM Host Server. Replaces the IP with Configuration NSM Host Server IP where the TCP/IP address of your 5500 Control Unit instead of TCPI-PADDR.

Appendix D. Special Notices

This publication is intended to help System Specialists and Business Partners who are assisting customers to implement an IBM Network Station solution for their network user needs. The information in this publication is not intended as the specification of any programming interfaces that are provided by the IBM Network Station and the Network Station Manager Program.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, NY 10594 USA.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The information about non-IBM ("vendor") products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere.

© Copyright IBM Corp. 1999

Customers attempting to adapt these techniques to their own environments do so at their own risk.

Any pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

Any performance data contained in this document was determined in a controlled environment, and therefore, the results that may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

The following document contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples contain the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Reference to PTF numbers that have not been released through the normal distribution process does not imply general availability. The purpose of including these reference numbers is to alert IBM customers to specific information relative to the implementation of the PTF when it becomes available to each customer according to the normal IBM PTF distribution process.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

AIX
AS/400
IBM ®
OS/400
RS/6000
400
APPN
DB2
Nways
RISC System/6000
S/390

The following terms are trademarks of other companies:

Citrix and Citrix MetaFrame are trademarks of Citrix Systems, Inc.

C-bus is a trademark of Corollary, Inc.

Java and HotJava are trademarks of Sun Microsystems, Incorporated.

Microsoft, Windows, Windows NT, and the Windows 95 logo are trademarks or registered trademarks of Microsoft Corporation.

PC Direct is a trademark of Ziff Communications Company and is used by IBM Corporation under license.

Pentium, MMX, ProShare, LANDesk, and ActionMedia are trademarks or registered trademarks of Intel Corporation in the U.S. and other countries.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Other company, product, and service names may be trademarks or service marks of others.

Appendix E. Related Publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

E.1 International Technical Support Organization Publications

For information on ordering these ITSO publications see “How to Get ITSO Redbooks” on page 291.

- *AS/400 - IBM Network Station - Getting Started*, SG24-2153
- *AS/400 Electronic-Mail Capabilities*, SG24-4703
- *AS/400 TCP/IP Auto Configuration: DNS and DHCP Support*, SG24-5147
- *AS/400 - IBM Network Station Printing*, SG24-5212
- *Lotus Domino for AS/400, Installation Customization, Administration*, SG24-5181
- *IBM Network Station Manager Release 3 Guide for Windows NT*, SG24-5221

E.2 Redbooks on CD-ROMs

Redbooks are also available on CD-ROMs. **Order a subscription** and receive updates 2-4 times a year.

CD-ROM Title	Subscription Number	Collection Kit Number
System/390 Redbooks Collection	SBOF-7201	SK2T-2177
Networking and Systems Management Redbooks Collection	SBOF-7370	SK2T-6022
Transaction Processing and Data Management Redbook	SBOF-7240	SK2T-8038
Lotus Redbooks Collection	SBOF-6899	SK2T-8039
Tivoli Redbooks Collection	SBOF-6898	SK2T-8044
AS/400 Redbooks Collection	SBOF-7270	SK2T-2849
RS/6000 Redbooks Collection (HTML, BkMgr)	SBOF-7230	SK2T-8040
RS/6000 Redbooks Collection (PostScript)	SBOF-7205	SK2T-8041
RS/6000 Redbooks Collection (PDF Format)	SBOF-8700	SK2T-8043
Application Development Redbooks Collection	SBOF-7290	SK2T-8037

© Copyright IBM Corp. 1999

E.3 Other Publications

These publications are also relevant as further information sources:

- *IBM 2212 Access Utility Introduction and Planning Guide*, GA27-4215
- *IBM 2212 Access Utility Installation and Initial Configuration Guide*, GA27-4216
- *Internet Connection Services and Internet Connection Secure Server for AS/400 Webmasters Guide,* GC41-5434
- *AS/400 - IBM Network Station Use*, SA41-0036
- *AS/400 - IBM Network Station Manager Installation and Use*, SC41-0664
- *TCP/IP Configuration and Reference*, SC41-5420
- *TCP/IP Fastpath*, SC41-5430
- RFC 826 - *Address Resolution Protocol*
- RCF 1027 - *Proxy ARP*

How to Get ITSO Redbooks

This section explains how both customers and IBM employees can find out about ITSO redbooks, CD-ROMs, workshops, and residencies. A form for ordering books and CD-ROMs is also provided.

This information was current at the time of publication, but is continually subject to change. The latest information may be found at `http://www.redbooks.ibm.com/`.

How IBM Employees Can Get ITSO Redbooks

Employees may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **Redbooks Web Site on the World Wide Web**

  `http://w3.itso.ibm.com/`

- **PUBORDER** – to order hardcopies in the United States
- **Tools Disks**

  To get LIST3820s of redbooks, type one of the following commands:

  ```
  TOOLCAT REDPRINT
  TOOLS SENDTO EHONE4 TOOLS2 REDPRINT GET SG24xxxx PACKAGE
  TOOLS SENDTO CANVM2 TOOLS REDPRINT GET SG24xxxx PACKAGE (Canadian users only)
  ```

  To get BookManager BOOKs of redbooks, type the following command:

  ```
  TOOLCAT REDBOOKS
  ```

  To get lists of redbooks, type the following command:

  ```
  TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET ITSOCAT TXT
  ```

  To register for information on workshops, residencies, and redbooks, type the following command:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ITSOREGI 1998
  ```

- **REDBOOKS Category on INEWS**
- **Online** – send orders to: USIB6FPL at IBMMAIL or DKIBMBSH at IBMMAIL

Redpieces

For information so current it is still in the process of being written, look at "Redpieces" on the Redbooks Web Site (`http://www.redbooks.ibm.com/redpieces.html`). Redpieces are redbooks in progress; not all redbooks become redpieces, and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

© Copyright IBM Corp. 1999

How Customers Can Get ITSO Redbooks

Customers may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **Online Orders** – send orders to:

	IBMMAIL	**Internet**
In United States	usib6fpl at ibmmail	usib6fpl@ibmmail.com
In Canada	caibmbkz at ibmmail	lmannix@vnet.ibm.com
Outside North America	dkibmbsh at ibmmail	bookshop@dk.ibm.com

- **Telephone Orders**

United States (toll free)	1-800-879-2755
Canada (toll free)	1-800-IBM-4YOU
Outside North America	(long distance charges apply)
(+45) 4810-1320 - Danish	(+45) 4810-1020 - German
(+45) 4810-1420 - Dutch	(+45) 4810-1620 - Italian
(+45) 4810-1540 - English	(+45) 4810-1270 - Norwegian
(+45) 4810-1670 - Finnish	(+45) 4810-1120 - Spanish
(+45) 4810-1220 - French	(+45) 4810-1170 - Swedish

- **Mail Orders** – send orders to:

IBM Publications Publications Customer Support P.O. Box 29570 Raleigh, NC 27626-0570 USA	IBM Publications 144-4th Avenue, S.W. Calgary, Alberta T2P 3N5 Canada	IBM Direct Services Sortemosevej 21 DK-3450 Allerød Denmark

- **Fax** – send orders to:

United States (toll free)	1-800-445-9269
Canada	1-800-267-4455
Outside North America	(+45) 48 14 2207 (long distance charge)

- **1-800-IBM-4FAX (United States)** or **(+1) 408 256 5422 (Outside USA)** – ask for:

  Index # 4421 Abstracts of new redbooks
  Index # 4422 IBM redbooks
  Index # 4420 Redbooks for last six months

- **On the World Wide Web**

Redbooks Web Site	http://www.redbooks.ibm.com
IBM Direct Publications Catalog	http://www.elink.ibmlink.ibm.com/pbl/pbl

Redpieces

For information so current it is still in the process of being written, look at "Redpieces" on the Redbooks Web Site (`http://www.redbooks.ibm.com/redpieces.html`). Redpieces are redbooks in progress; not all redbooks become redpieces, and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

IBM Redbook Order Form

Please send me the following:

Title	Order Number	Quantity

First name	Last name	
Company		
Address		
City	Postal code	Country
Telephone number	Telefax number	VAT number

☐ Invoice to customer number _____

☐ Credit card number _____

Credit card expiration date	Card issued to	Signature

We accept American Express, Diners, Eurocard, Master Card, and Visa. Payment by credit card not available in all countries. Signature mandatory for credit card payment.

Index

Symbols

. 207

A

Access Integration Services (AIS) 26
AIS (Access Integration Services) 26
applet viewer 5
ASCII 16
authentication server, decentralized 217

B

boot
  broadcast 3, 10
  flash memory 28
  peer (buddy) 3
  sequence 107
  storms 10
boot image
  creation 73
  loading 82
  testing 73
booting
  peer 96
browser
  NC Navigator 3
  web access 243

C

centralized authentication server 213
  defaults.dft 216
Citrix 14
co-existence CISC/RISC 57
configuration
  AS/400 IP 132
  centralized 121
  eSuite mail 231
  mail 225
  POP3 225
  twinax connection 131

D

datastream, transferring 16
DHCP
  MAC addresses 21
  remote 171
  twinax 154
display, touch screen 3
distributed site model 124
Domino 239
  server conflicts 242

E

emulator
  AS/400 5
  S/390 5
emulators
  3270 3
  5250 3
  VT100 14
  VT102 14
  VT200 14
  VT220 14
  Vt300 14
  VTxx Telnet 3
eSuite 228, 231
  station 229
executable module 267

F

file manager
  commands 86
  local 86
flash boot network station configuration 100
flash card
  3270 65
  5250 65
  ACTLogin 65
  boot image 65
  booting network station 89
  copying from NFS 82
  creation 65
  emulation 255
  formatting 82
  housekeeping 91
  loading 82
  management 65
  sizing 65
  VTxxx 65
flash cards 3, 63, 255
  centennial 63

© Copyright IBM Corp. 1999

part numbers 63
PCMCIA 63
simple technology 63
flash memory card 28
FLASH.NSM 261
fonts, emulators 258

G

group preferences creation sample 221

H

HTTP server 242

I

IBM Network Station
overview 1
IBM Network Station Manager
omitting default menu bar buttons 219
prerequisite PTFs 215
replicating to remote server 214
ICA
support 264
X11 17
initialization
BOOTP 42
mechanisms 40
options 22
Integrated PC Server (IPCS) 14
IPCS (Integrated PC Server) 14

J

Java 2
support 265
Java Virtual Machine
NC Navigator 262
Java Virtual Machine (JVM) 2, 262
JVM (Java Virtual Machine) 2, 262

K

kernal 10
kiosk 3

L

local file manager
NFS 81
Lotus
eSuite workplace 228
Lotus Notes installation 250

M

mail, accessing from Network Station 225
management
capacity 36
change 55
performance 36
problem 55
remote sites 121
MetaFrame 14
migration considerations 55

N

National Language Support (NLS) 4
NC Navigator 234
configuring 235
Network
Ethernet 4
Token Ring 4
Network Station
booting from flash 90
eSuite 229
eSuite mail 231
file manager 86
local file manager commands 88
mail access 225
Series 100 1
Series 1000 2
Series 300 2
TSE connection 249
twinax attached 127
use of twinax 127
Network Station Manager
group support 5
NFS, copying data 82
NLS 4
NVRAM 36
local boot modifications 91

O

Operator Information Area 13

P

PCL 16
PCMCIA

adapter 4
memory card 28
slot 4
peer boot
configuration file 101
network topology 97
PEER.NSM 261
performance
5250 applications 44
AS/400 router 50
browser 50
flash card peer boot 55
JVM 50
slow link boot 55
TFTP jobs 44
POP3 225
configurations 225
PostScript 16
print
LPR/LPD 3
printing 15
administration 58
basics 58
configuring 58
scenarios 58
problem determination 209
console log 209
system log 209
Proxy AR 145

R

remote boot server
replicate 213
replicating 213
replication, decentralized authentication
STRNSSA 222
remote servers 107
remote sites, managing user configuration 121
replicating 213
replicating remote boot servers
transferring IFS directories 223
replication, remote boot server 213
roaming 120
function 7
router 26
AS/400 performance 51

S

separation of servers 6, 65
server
authentication 6
base code 6
BOOTP/DHCP 6
centralized 213
local DHCP 154
remote access 26
remote boot 191
remote DHCP 171
replicator 213
terminal configurator 6
server consolidation 109
servers
Citrix 248
Domino 242
HTTP 242
metaframe 248
remote 107
remote boot 22
separater 6
separation of 3
split boot 107
TSE 248
service levels 33
setting 243
setup
hardware 10
workstation 10
split boot servers 107
STRNSSA, centralized authentication (remote boot server replication) 216
subnet 10
address pool 187
subnetting
transparent 141
twinax 141

T

TCP/IP 24
addressing 146
TDLC (Twinax Data Link Control) 15
Terminal Server Edition (TSE) 14, 248
transparent subnetting
twinax 141
Trivial File Transfer Protocol (TFTP) 10
TSE (Terminal Server Edition 14, 248

twinax 3
advanced IP 144
attached network stations 127
basic IP 128
DHCP 154
remote boot 191
remote DHCP 171
Twinax Data Link Control (TDLC) 15
twinax subnet address pool 187

U

user configuration management 121
users
local 21
remote 21

V

Views 245

W

WinCenter 14

ITSO Redbook Evaluation

AS/400 IBM Network Station: Techniques for Deployment in a WAN
SG24-5187-00

Your feedback is very important to help us maintain the quality of ITSO redbooks. **Please complete this questionnaire and return it using one of the following methods:**

- Use the online evaluation form found at http://www.redbooks.ibm.com
- Fax this form to: USA International Access Code + 1 914 432 8264
- Send your comments in an Internet note to redbook@us.ibm.com

Which of the following best describes you?
_ **Customer** _ **Business Partner** _ **Solution Developer** _ **IBM employee**
_ **None of the above**

Please rate your overall satisfaction with this book using the scale:
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction _____

Please answer the following questions:

Was this redbook published in time for your needs? Yes___ No___

If no, please explain:

_____

_____

_____

_____

What other redbooks would you like to see published?

_____

_____

_____

Comments/Suggestions: (THANK YOU FOR YOUR FEEDBACK!)

_____

_____

_____

_____

© Copyright IBM Corp. 1999

SG24-5187-00
Printed in the U.S.A.

AS/400 IBM Network Station: Techniques for Deployment in a WAN

SG24-5187-00